جرائم تكنولوجيا المعلومات

- رؤية جديدة للجريمة الحديثة -

تأليف

جعفر حسن جاسم الطائي

ماجستير مكتبات ومعلومات

جامعة عمر المختار

قسم المكتبات والمعلومات - البيضاء

الطبعة الأولى

٢٠٠٧م - ١٤٢٨ هـ



جرائم تكنولوجيا المعلومات

- رؤية جديدة للجريمة الحديثة -

تأليف

جعفر حسن جاسم الطائي

ماجستير مكتبات ومعلومات

جامعة عمر المختار

قسم المكتبات والمعلومات - البيضاء

الطبعة الأولى

٢٠٠٧م - ١٤٢٨ هـ



دار البداية ناشرون وموزعون

رقم الإيداع لدى دائرة المكتبة الوطنية (٢٠٠٧/١/١٣)

٣١٤.٠٤٨

الطائي، جعفر

جرائم تكنولوجيا المعلومات:رؤية جديدة للجريمة الحديثة/ جعفر حسن جاسم الطائي - عمان : دار البداية، ٢٠٠٧

(   ) ص

ر.أ: (٢٠٠٧/١/١٣)

الواصفات: /الجريمة//تكنولوجيا المعلومات//علم الجريمة

* تم إعداد بيانات الفهرسة والتصنيف الأولية من قبل دائرة المكتبة الوطنية.

الطبعة العربية الأولى

٢٠٠٧م - ١٤٢٧هـ



دار البداية ناشرون وموزعون

عمّان - شارع الملك حسين - مجمع الفحيص التجاري

هاتف: ٤٦٤٠٦٧٩ - تلفاكس: ٤٦٤٠٥٩٧

ص.ب ٥١٠٣٣٦ عمان ١١١٥١ الأردن

إهداء

إلى التي قدمت لي آيات الحب والحنان في أواني الدموع مع أمـواج البحـار المتلاطمة، مع بسمة كل صباح وشهقة كل غروب، آهاتها الممزوجة بالدعاء.



إلى أجمل وردة في بستاني....

إلى أعذب كلمة ردّدها لساني

إلى من وضعت الجنة تحت أقدامها....

إلى من ملأ الحنان وجدانها

إلى من وهبتني حياتها.... ورضاها أمل حياتي

إلى قلبي وهي قلبي.... ودعواتها تنير دربي

إلى أسرتي المعطاء

زوجتي

وأولادي

زينب

صادق

أول من يجب له الشكر والثناء هو الـلـه ربنا، فقد استعنت به فكان نعم المستعان. إذ لا يسعني وأنا أنجز كتابي هذا إلا أن أشكر الـلـه على جزيل رحمته وتوفيقه لإكمال مهمتي.

يسعدني ويشرفني أن أقدم جزيل شكري وامتناني إلى الأخ والصديق الدكتور

محمد عبد الرضا شياع الذي أنار لي درب الكتابة من خلال فتح نافذة آفاقها الواسعة، دعائي له عند كل صباح ومساء بدوام الصحة والتوفيق.

شكر وتقدير

كما يسعدني وأنا أضع اللمسات الأخيرة على هـذا العمـل المتواضـع بـأن أقـدم شـكري وتقـديري إلى جميـع العـاملين والقـائمين في المكتبـة المركزيـة بجامعة عمر المختار.

وأتقدم بشكري وامتناني وتقديري إلى الدكتور

عباس غالي الحديثي لما أبداه من حسن التعاون.

قبل الختام أتقدم بدعائي وتوفيقي وشكري وامتناني إلى الشعب العربي الليبي الكريم، وإلى كل الأخوة والأخوات والسادة المسؤولين في كليـة الآداب والعلوم في جامعة الجبل الغربي، وإلى الأخوة والأخوات والسادة المسؤولين في جامعة عمر المختار راجياً ومتمنياً من الـلـه أن يحفظ الجميع من كل سوء.

وفي الختام لا يسعني إلا أن أزجي شكري المتواصل لكل من آزرني ومد يد العون والمساعدة على إنجاز هذه المهمة العلمية، متمنياً للجميع دوام التقدم والتوفيق. و الـلـه الموفق.

جعفـــر حســن جاســم الطائـــي

مقدمـــــة

أدى التطور الحضاري الذي أنجزه الإنسان في مجالات الحياة المختلفة، ومنها مجال تكنولوجيا المعلومات إلى دخـول الإنسانية عصراً جديداً لم تألفه من قبل في حياتها. لقد انعكست نتائج استخدام تكنولوجيا المعلومات على المجتمعات الحديثة، وأظهرت للعيان وبشكل واضح وملموس تأثيراً كبيراً ليس في سلوكيات الإنسان فحسب، بل وفي تأثيرها على طريقة تفكيره من جهة، وطريقة عمله من جهة ثانية.

لقد أصبحت تكنولوجيا المعلومات اليوم تمثل سمة من سمات العصر الراهن، وبالتالي بات لزاماً على كل مجتمع يريد أن يتعايش، بل ويتواصل مع المجتمعات الأخرى، عليه أن لا يجهل أو يتجاهل أهميتها أو يعيش بدونها، أضف على ذلك: أن التطور الحاصل في عالم تكنولوجيا المعلومات، بات يدعو إلى التأمل والتوقف إزاء هذه الظاهرة التكنولوجية، أكثر مما يدعو للدهشة. لقد باتت تكنولوجيا المعلومات الرئة الجديدة التي يتنفس منها أبناء مجتمع المعلومات العالمي، لا بل أصبحت القلب النابض للإنسان.

بناءً على ما تقدم، صار لزاماً ولكي نحدث تغييراً جذرياً في مسارنا التاريخي لا بد أن نستوعب عناصر التغيير الفعال لا سيما التي تؤسس طريق المستقبل وبشكل أخص العناصر المستحدثة، وإلا فإن العنصر قد ينقلب إلى أزمة حقيقية إن لم يُفهم ويتعامل معه بشكل جيد، ومن هذه التحديات التاريخية الجديدة ظاهرة المعلوماتية التي فرضت نفسها بوصفها عنصر حاسم في صراع الأمم وصياغة المستقبل وامتلاك الغد القريب والبعيد، ويجب أن نفهم جميعاً، إن هذه الظاهرة سوف تستأصلنا إن لم نستوعبها وننتزع أنيابها، كما أنها يمكن أن تكون عنصر تغيير بناء للمستقبل إن استفدنا من جوانبها الإيجابية.

لا يستطيع أحد أن يتجاهل التغييرات الجوهرية التي أحدثتها ثورة تكنولوجيا المعلومات في المجالات الاقتصادية والاجتماعية والسياسية. فقد قلبت العديد من المعطيات الاجتماعية والاقتصادية وموازين القوى المجتمعية التي أثـرّت سلباً وإيجاباً على الأوضاع العامة للمجتمعات الصناعية وغير الصناعية، ومن أهم التغييرات التي أحدثتها الثورة المعلوماتية تغير الوضع الاجتماعي والاقتصادي والمهني لأفراد المجتمع لاسيما الأسرة.

وفق المعطيات السابقة، باتت تختلف نظرة الناس نحو تكنولوجيا المعلومات الجديدة، ففي الوقت الذي تبعث فيه على الإعجاب في نفوس العديدين عند الاستفادة منها في علاج مشكلات عديدة، إلا أنها تبدو مروعة، لاسيما عندما يتعلق الأمر بتهديد أمن وحياة المجتمعات.

فتكنولوجيا المعلومات بوصفها أداة للربط والاتصال والتخزين والاسترجاع بين الناس في مختلف أرجاء الأرض، باتت تشكل أداة ليس للبحث عن المعلومة فحسب، بل وتوظيف هذه المعلومة لأغراض الجريمة، والأكثر من ذلك، إنها أضحت تمثل مكاناً جغرافياً لارتكاب الجرائم، لاسيما الجرائم المعلوماتية منها تحديداً؛ وذلك من حيث إساءة استخدام تكنولوجيا المعلومات، والعمل على توظيفها سلبياً وبشكل غير قانوني، لإشباع رغبات النفس الإنسانية، وكل تلك الرغبات الإنسانية غير المشروعة ولَّدت جرائم جديدة لم تكن مألوفة لدى المجتمع ويمكن أن نطلق عليها جرائم تكنولوجيا المعلومات، أو أحياناً أخرى تسمى الجرائم المعلوماتية.

لذلك تبقى الأسئلة القلقة التي تهز مضاجع العديد من أبناء المجتمع هي تلك التي تتعلق بطبيعة هذا العصر الذي لقب بعصر المعلومات ومرة أخرى بعصر تكنولوجيا المعلومات. وأفرزت هذه التكنولوجيا، العديد من المعطيات الإيجابية والسلبية على حدٍ سواء، لعل الإيجابيات ينتفع منها الناس دون معرفتهم بها أحياناً، بيد أن السلبيات هي التي يجب التنويه عنها لكي يأخذ الناس حذرهم منها، وفي مقدمة تلك السلبيات التي يجب إظهارها تلك التي تتعلق بجرائم تكنولوجيا المعلومات، ولكي لا تبقى الرؤية ضبابية أمام أبناء المجتمع، كان لا بد من الإفصاح عن تلك الجرائم، وتبقى الأسئلة التي تحتاج إلى قبس الإفصاح عنها جرائم تكنولوجيا المعلومات؟ وكيف تحدث جرائم تكنولوجيا المعلومات؟ وما السبيل لمكافحة تلك الجرائم؟

من هنا جاء هذا الكتاب الذي يحمل عنوان "جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة"، ليقدم ولَدَتها تكنولوجيا المعلومات.

لقد قسمّ الكتاب على خمسة فصول، جاء الفصل الأول منها بعنوان (ظاهرة الجريمة في المجتمع)، وقد اشتمل على (٥) فقرات، الأولى تتحدث عن ظاهرة الجريمة من منظور تاريخي، أما الفقرة الثانية تضمنت "مفهوم الجريمة والمفاهيم ذات العلاقة"، في حين اشتملت الفقرة الثالثة على " تصنيف المجرمين"، أما الفقرة الرابعة فقد تضمنت على "تصنيف الجرائم"، في حين الفقرة الخامسة فتضمنت على "الأسباب والدوافع والعوامل وراء ظاهرة الجريمة".

بينما يتناول الفصل الثاني (تكنولوجيا المعلومات: المخاوف والهموم والمخاطر) فقد اشتمل على (٥) فقرات، الأولى كانت "تكنولوجيا المعلومات والتحدي الاجتماعي"، والثانية "تكنولوجيا المعلومات المخاوف والهموم"، والثالثة "تكنولوجيا المعلومات تدق ناقوس الخطر"، والرابعة "جحيم تكنولوجيا المعلومات المرفوض"، والخامسة "تكنولوجيا الإعلام وتأثيرها على سلوك الأفراد".

أما الفصل الثالث جاء بعنوان (ظاهرة جرائم تكنولوجيا المعلومات: التعريف والتاريخ والخصائص والتصنيف)، فقد تضمن على (٨) أجزاء، الأول: "ظاهرة جرائم تكنولوجيا المعلومات والتسميات المتعددة"، أما الثاني " تعريف جرائم تكنولوجيا المعلومات"، والثالث "ظاهرة جرائم تكنولوجيا المعلومات: التاريخ والخسائر"، والرابع " ظاهرة جرائم تكنولوجيا المعلومات والخسائر: أرقام وتواريخ"، أما الجزء الخامس فكان "ما تقسيمات جرائم تكنولوجيا المعلومات؟"، والسادس " ما أسس وأنواع جرائم تكنولوجيا المعلومات؟"، والسابع "خصائص وسمات جرائم تكنولوجيا المعلومات"، والجزء الأخير كان " أسباب انتشار جرائم تكنولوجيا المعلومات".

جاء الفصل الرابع بعنوان (جرائم تكنولوجيا المعلومات: مقترفوها ، أساليب ارتكابها، أنواعها)، اشتمل على (٦) فقرات، الأولى "من الذي يرتكب جرائم تكنولوجيا المعلومات؟"، والثانية أشارت إلى " الدوافع وراء ارتكاب جرائم تكنولوجيا المعلومات"، أما الثالثة فقد أشارت " الظروف البيئية لارتكاب جرائم تكنولوجيا المعلومات"، والرابعة تضمنت "كيف يتم ارتكاب جرائم تكنولوجيا؟"، في حين الفقرة الخامسة أشارت إلى " أساليب ارتكاب جرائم تكنولوجيا المعلومات". والسادسة بيّنت "أنواع جرائم تكنولوجيا المعلومات".

بينما يتناول الفصل الخامس والأخير (مكافحة جرائم تكنولوجيا المعلومات) فقد اشتمل على شقين: الشق الأول يتحدث عن "المشكلات التي تقف وراء صعوبة المكافحة، في حين اشتمل الشق الثاني على " طرق وأساليب مكافحة جرائم تكنولوجيا المعلومات".

وبعد : فإن هذا الكتاب هو جهد متواضع أضعه بين يدي القارئ العربي في وطننا العزيز، فهذا (الكتاب يهم بالدرجة الأولى القارئ والمتعلم والمثقف العربي، وبشكل أخص طلاب علم الاجتماع والقانون وعلم النفس ، مضافاً عليهم رجال القانون والأمن وجميع المراقبين والمهتمين والمعنيين بشؤون المجتمع، راجياً أن يكون بقعة ضوء في زمن التعتيم. ويحدوني الأمل في أن يجد كل أولئك متعة وفائدة، وأتمنى أن ينال إعجاب ورضا القراء.

و الله ولي التوفيق

جعفـــر جاسم الطائــي

البيضاء - الجماهيرية الليبية

٢٠٠٦

الفصل الأول




ظاهرة الجريمة في المجتمع العربي

تقديم

يقيناً إن الذات الإنسانية تبقى تبحث عن ماهية وملامح المجتمع السعيد، سواء كانت تلك المجتمعات متخلفة أم متقدمة، ريفية أم حضرية، بيد أن هذه الذات تريد أن تفك حالة الالتباس والغموض التي تكشف حالة المجتمعات، قديمها وحديثها، وقبل هذا وذاك، ظلت النفس الإنسانية هي من بين أكثر الأمور المعقدة التي واجهت الإنسان أيما حل وارتحل، وكان فهم الإنسان لذاته موضع اهتمام علماء الاجتماع والنفس، ورغم تقدم العلوم في هذين المجالين، إلا أن الفهم العميق للذات الإنسانية، ما زال قاصراً، ولم يصل بعد إلى مرحلة النضوج النهائي.

علاوة على ذلك، فإن هناك ظواهر أخرى ما زالت معقدة وتقف في مقدمة تلك الظواهر، ظاهرة الجريمة، بوصفها واحدة من أهم الأمور البالغة التعقيد والملازمة للمجتمعات الإنسانية، حيث أن المجتمعات البشرية عرفت الجريمة، وظلت ملازمة لها حتى يوم الناس هذا، وطالما أن الأمر كذلك، فإن العديد من المتخصصين باتوا يطلقون عليها أو يصفونها بأنها "ظاهرة طبيعية" فهل هي كذلك؟ فلنتبين من ذلك.

١- ظاهرة الجريمة: منظور تاريخي.

لقد بات مؤكداً من خلال دراسة تاريخ المجتمعات الإنسانية، أن ظاهرة الجريمة هي ليست وليدة العصر الحاضر، بل إنها قديمة قدم الوجود الإنساني. لقد لازمت الظاهرة الإجرامية المجتمع الإنساني عبر رحلته في الزمان والمكان المختلفين، فأينما حلّ وارتحل الإنسان، حلّت معه أحلامه، وأطماعه، المشروعة وغير المشروعة، ولم يعش أي مجتمع من المجتمعات قديمها وحديثها، خالٍ من ظاهرة الجريمة، فكان لكل مجتمع نصيب من ظاهرة الجريمة.

لقد ظهرت الجريمة منذ أن ظهر الإنسان على سطح الأرض، وكان قتل قابيل لأخيه هابيل أول جريمة عرفتها البشرية. ومن هنا كانت الحاجة للتفسير. وحين استشعر الأفراد بحاجتهم إلى التعاون فيما بينهم والانضواء تحت شكل من أشكال التنظيم الاجتماعي، صار لزاماً عليهم كبح جماح رغباتهم، واحد من بعض نزعاتهم الأنانية التي تلحق ضرراً بالتنظيم الاجتماعي الذي ينتسبون إليه. وفي هذه المرحلة لم تكن قد ظهرت بعد فكرة البحث عن تفسير للجريمة. وكانت الجرائم المعروفة آنذاك هي القتل والجرح والضرب. كما عرفت الجرائم التي تمس حرمة المعتقدات الدينية كالسحر ونبذ الآلهة أو الخروج عن التعاليم الدينية بوجه عام (١).

من أجل تسليط الضوء على الخلفية التاريخية للجريمة، يتطلب الأمر العودة إلى البدايات الأولى لمسألة (التحريم)، لقد عرفت المجتمعات منذ قديم الزمان فكرة التحريم، من المعروف أن لكل إنسان حاجات ودوافع وغرائز أولية وأخرى مكتسبة لا بد من إشباعها، بيد أن وجوده في جماعة أصبح لزاماً عليه أن يكف من حاجاته، ونزعاته، ويعد لها إذا حدث تعارضاً بين هذه الحاجات والنزعات، وبينها وبين نزعات الجماعة أو الأفراد الآخرين أو قد ينشأ الصراع بين الفرد والمجتمع أو بين الفرد والآخر، وذلك في حالة عجز الفرد عن التوفيق بين حاجاته وما يتطلبه منه المجتمع. والواقع أن عملية التوفيق هذه اقتضت من الإنسان أن يكف بعض نزعاته الفردية، أي أن يحرم بعض الأمور على نفسه، واقتضت من المجتمع أن يتدخل بما يضعه من قواعد تعين الإنسان على كف نزعاته التي لا يرضاها المجتمع، وهذه القواعد تشمل النظم الاجتماعية التي سنّها المجتمع لنفسه من عادات، وعرف، وتقاليد، وقضاء، وغير ذلك من الأحكام والقيم السلوكية المختلفة وذلك بقصد مجابهة مشكلات الإنسان والتخفيف من حدّة الصراع بين الإنسان والآخر وبينه وبين البيئة الاجتماعية التي يعيش فيها، وهذا هو الأصل في التحريم حتى يضمن الإنسان حياته وبقاؤه، وحتى يستطيع أن يشبع حاجاته بطريقة لا تتعارض مع غيره، والأفعال التي تتدخل فيها الدولة أو السلطة الحاكمة عادة لتأكيد حرمتها بالتهديد والقوة أو بعبارة أخرى باستعمال السلطة وبسن القوانين ليست إلا جانباً من المحرمات التي يشملها النظام الديني أو مبادئ الأخلاق والعرف والتقاليد السائدة في المجتمع.

عرف التحريم منذ نشأة المجتمعات الإنسانية، وكان التحريم في المجتمعات البدائية البسيطة ملتصقاً بالنظام الديني لها، فقد كانت كل عشيرة أو قبيلة تلتف حول رمز إلهي غالباً ما يكون حيواناً أو نباتاً و"التوتم"، تعتقد العشيرة أنها تنحدر من سلالته، ويتضمن هذا النظام " التوتمي" طقوساً دينية يتعين أداؤها للتوتم، وأفعالاً وأشياءً يحرم إقترافها أو الاقتراب منها أو المساس بها هي "التابو"، ويتخلل التابو كل النظم الاجتماعية التي تسير عليها الجماعة، ويشاهد في جميع نواحي الحياة والموت، كالعبادة والحياة الجنسية والأسرة والصيد والمرض والطعام.

أضف إلى ذلك: فإن من قواعد التابو هذه تحريم أكل حيوان معين، وتحريم حضور الحفلات الدينية على النساء، وتحريم النطق بأسماء الموتى والامتناع عن تصرفات معينة قبل الخروج للحرب أو القنص، ويستند التابو عادة إلى القداسة والنجاسة، فالشيء النجس كالشيء المقدس، كلاهما سواء في حكمه، فبينما نرى أن زعيم القبيلة (تابو) يحرم المساس به من باب القداسة،

نجد أن المرأة الحائض هي الأخرى (تابو) لا تمس ولا يمس أي شيء مسته، وكلاهما يلقى الرهبة والخوف في قلب الإنسان، وتكتنفه الأسرار والإيمان بالأرواح والأشباح والقوى الغامضة.

هكذا نرى أن المجتمعات البدائية عرفت صور التحريم، وأن التحريم في المجتمعات البدائية التصق بالدين وأن الدين كان أول مصدر من مصادر التحريم بوصفه قواعد لها صفات غيبية تعمل على تنظيم صلة الإنسان بمن يعبد وصلة الإنسان بالإنسان. وإذا كانت فكرة التحريم في مثل هذه الصورة البدائية لم تعرف إلا في المجتمعات الوثنية البدائية، فإن فكرة التحريم ظلت متصلة بالدين اتصالاً وثيقاً، فقد جاءت ونادت بفكرة الثواب والعقاب والقصاص، وساعدت كثيراً على تأكيد العديد من المحرمات وتحديدها، وفكرة الاتصال بين الدين والجريمة ما زالت مظاهرها تتضح في اعتبار الأفعال الموجهة ضد الدين أو العقائد الدينية أو المساس بها كالإلحاد، والكفر، والشعوذة، أفعالاً إجرامية تستوجب العقوبة، إلا أن هذه الصلة بين الجريمة والدين أخذت تضعف بنهاية العصور الوسطى وانتكاس الإيمان الديني في العصر الحديث (٢).

علاوة على ذلك، فإن الدين يعد من أهم مصادر التحريم وأقواها أثراً في حياة الجماعة، كذلك تعتبر الأخلاق مصدراً هاماً من مصادر التحريم، ويعد التحريم خلقياً إذا استند إلى قاعدة خلقية تصف الأفعال أو النوايا بأنها خير أو شر. فالأخلاق عبارة عن قواعد مقبولة من المجتمع ومعترف بها وأساسها التفريق بين الخير والشر، وهي قواعد تأمر وتحث وتستلزم بذل الجهد في قهر النفس، كما تتضمن من ناحية أخرى الخوف من غضب الجماعة واستنكارها، والضمير الخلقي هو الأساس في استلزام القاعدة الخلقية، كما أن القاعدة الخلقية كثيراً ما تكون مستمدة من البيئة أو مرتبطة بها، وفي هذه الحالة تزداد قوة. ونلاحظ أنه لا يمكن الفصل بين الدين والخلق إذ أنهما اقترنا سوياً وامتزجا سوياً حتى يصعب فصل أحدهما عن الآخر فصلاً تاماً.

يمكن القول: إنه بتعقد الحياة الاجتماعية وتطورها، بدأت السلطة الحاكمة تتدخل بنفوذها وقوتها لتؤكد تحريم جانباً من المحرمات عن طريق القانون غير قانعة بأن الدين ينهي عن إثباتها ويهدد مقترفيها بالعقاب في الآخرة أو أنها تتنافى مع الأخلاق، ومع ذلك فالقانون يترك للدين والأخلاق أموراً كثيرة لا يتعرض لها وخاصة الأفعال المتعلقة بالنوايا والتي يصعب إثباتها، ويقتصر على الأفعال المادية التي يمكن إثباتها (٣).

إذا كانت العادات والتقاليد والأعراف تشير إلى ما يسمى بـ (المحرمات)، فإن القانون بدأ يشير إلى مفهوم جديد هو (الجريمة)، وتؤكد مصادر المعلومات أن ظاهرة الجريمة قديمة العهد عند

الصغار والكبار، فالجريمة في المجتمع ليست ظاهرة حديثة العهد، بل عانت منها المجتمعات القديمة وعرفتها التشريعات في مختلف العصور عن طريق منع إرتكاب بعض الأفعال التي تشكل إضطراباً وخطورة على المجتمع والعلاقات السائدة فيهن وذلك منذ أن شرع الإنسان يعيش في نطاق العشيرة أو القبيلة رغم عدم وجود سلطات رسمية في بادئ الأمر كالبوليس والمحاكم والسجون.

فالمجتمعات لم تخل تماماً من الجريمة فهي نتيجة لازمة لحياة الناس وما يثور بينهم من تنازعٍ في المصالح وتنافس على إشباع الحاجات (٤).

١- كيف ينظر المجتمع إلى ظاهرة الجريمة عبر التاريخ؟

يبقى السؤال المهم هنا مفاده : كيف ينظر المجتمع إلى ظاهرة الجريمة؟ تأتي الإجابة فتخبرنا بأن النظرة الاجتماعية ترى أن مفهوم الجريمة كمخالفة للقانون ما هو إلا مخالفة لنوع معين من القوانين السلوكية السائدة في المجتمع، ومعنى ذلك أن هناك أنواعاً من السلوك يحرمها المجتمع على أفراده، وأن المجتمع في تحريمه لهذا النوع من السلوك يراعي مصالحه وأمنه واستقراره، وهي بهذا المفهوم ظاهرة اجتماعية وجدت في كافة المجتمعات البشرية قديمها وحديثها.

يقوم أي مجتمع من المجتمعات على مجموعة من النظم والقواعد الاجتماعية في مختلف نواحي النشاط الاجتماعي والعلاقات الاجتماعية التي تربط بين أفراد المجتمع، وهذا التنظيم الاجتماعي اصطنعته المجتمعات لنفسها تلقائياً وتعارفت عليه بقصد تنظيم إشباع حاجات الأفراد الاجتماعية، وتحقيق الصور المختلفة من الحقوق والواجبات، وبذلك فهو الأساس الذي ترتكز عليه الحياة الجماعية، وهو الذي ينظم علاقاتهم وبدونه يسود المجتمع فوضى تقضي عليه.

أما عملية التنظيم الاجتماعي: فهي عبارة عن مجموعة القواعد التي تعارف عليها المجتمع والتي تقوم بتنظيم سلوك أفراده مثل العادات والتقاليد والقانون والرأي العام، التي يلتزم الأفراد بإتباعها في حياتهم الجماعية، وكل من يخرج على هذا التنظيم بما يتضمنه من قواعد مختلفة يعتبر خارجاً على الجماعة، ومنحرفاً عن الطريق يقابل سلوكه هذا بأنواع معينة من الجزاء، الغرض منه ردع المخالف وردع غيره من معاودة هذا السلوك، كما يرى العقاب أن التوازن إلى الجماعة الذي اختل بسبب السلوك المخالف، وتتفاوت درجات الجزاء تبعاً لنوع السلوك ومدى ضَرَرَهُ أو نفعه بالنسبة للجماعة ووفقاً لمعتقداتها الخاصة بأنماط السلوك، كما يعمل المجتمع من جانبه على تصحيح الأوضاع التي نتجت عن هذا الخروج على قواعد الجماعة متى كان ذلك مستطاعاً حتى تعود الأمور سيرتها العادية.

وفق المعطيات السابقة، يمكنا القول: بأن الجريمة أو الانحراف هو نوع من أنواع الخروج على قواعد السلوك التي يرسمها المجتمع لأفراده، فالمجتمع هو الذي يحدد ماهية السلوك السوي وماهية السلوك المنحرف أو الإجرامي وفق القيم الاجتماعية التي رسمها لنفسه، وعلى ذلك فالجريمة نسبية تختلف من مجتمع لآخر ومن عصر لآخر، فوأد البنات في الجاهلية لم يكن يعتبر سلوكاً إجرامياً في ذلك الوقت بينما اعتبر جريمة بمجيء الإسلام والإجهاض يعتبر جريمة في المجتمع المصري، بينما لا يعتبر كذلك في بعض بلاد أوربا ما دام برغبة الأم (٥).

أضف على ذلك، فإن النظرة لمفهوم ظاهرة الجريمة، تبقى مختلفة تمام الاختلاف من حيث أنواعها، ومن حيث سلوكها. فالجريمة كظاهرة اجتماعية لها صور مختلفة، وأنواع متعددة، وتدل على أنواع متباينة من السلوك وليس على نوع واحد مثلها في ذلك، مثل مفهوم المرض لا يدل على حالة معينة بذاتها، بل له عدة أنواع. كذلك يلاحظ نتيجة لتعمد الحياة المدنية الحديثة والتطورات المختلفة التي مرّ بها المجتمع البشري في النواحي الاقتصادية والاجتماعية الصناعية والنقل والمواصلات وغير ذلك ظهر أنواع جديدة من الجريمة لم تكن معروفة من قبل.

بين هذا وذاك، يمكننا القول: بأن مفهوم الجريمة من الناحية الاجتماعية، وكذلك النظر إليها وفق هذا المنظور (الاجتماعي)، أنها عبارة عن نمط معين أو أنماط معينة من السلوك البشري، ترى الجماعة أو المجتمع أن فيه خروج على قواعدها التي تعارفت عليها لتنظيم حياتها الجماعية. وذلك متى رأت الجماعة في ذلك ضرر بمصلحتها الاجتماعية وتهديد لأمنها واستقرارها وتطورها. وأن هذه القواعد من السلوك التي سنتها المجتمعات لنفسها هي ما اتفق على تسميتها بالمحرمات التي يحرمها المجتمع على أفراده، وهي تخضع لشتى النواحي المؤثرة في المجتمع، وأن ما يعتبر محرماً في مجتمع لا يعتبر بالضرورة كذلك في مجتمع آخر؛ وذلك بالرغم من وجود بعض الجرائم التي تكاد تحرمها كل المجتمعات البشرية مثل القتل والسرقة، كما أن تحريم الفعل أو تجريمه يختلف من عصر لآخر حسب التطورات المختلفة التي يمر بها المجتمع في شتّى مجالات الحياة الاجتماعية والاقتصادية والحضارية... الخ (٦).

في ضوء المعطيات السابقة، ومن أجل إماطة اللثام عن تاريخ الجريمة بشكل واضح ومعمّق، يتطلب الأمر كشف النقاب عن ماهية الروح أو النفس الإنسانية، وفوق هذا وذاك يمكننا القول: إن ظاهرة الجريمة في المجتمع ليست حدثاً طارئاً، ولا تتوقف على ظرف من الظروف، لكنها قدر يلم بأغوارً النفسّ، فهي السلوك الناتج عن الصراع الداخلي والصراع مع المجتمع، وعن الإحباط،

هذا السلوك الذي اتخذ اتجاهاً لا يقره القانون . وسواء أكانت الجريمة ثمرة الفشل في تحقيق الانسجام النفسي بين الفرد والبيئة، أم ثمرة عجز البيئة عن توفير الإرضاء الملائم للفرد، فإنها عرض لصراع داخلي موجه ضد القانون الساري (٧).

تبقى ظاهرة الجريمة وإلى يوم الناس هذا، تشكل حالة من الغموض والالتباس، بل إنها ما زالت تمثل لغزاً للمجتمع الإنساني، ولهذا، فإنها ما زالت موضع اهتمام علماء الاجتماع وعلم النفس وكذلك علماء القانون، وكل المعنيين بشؤون المجتمعات من رجالات الأمن وأجهزتها المختلفة، إلا أن تحدي الجريمة لم يقف عند هذا الحد، بل إن تطور المجتمعات أضاف تحدياً جديداً للبشرية، تجسد هذا التحدي بظهور نوع جديد من الجرائم يضاف على الجرائم السابقة، إنها جرائم تكنولوجيا المعلومات.

٢- مفهوم الجريمة والمفاهيم ذات العلاقة:

من أجل تحديد مفهوم الجريمة والتعريف بها، يتطلب الأمر، تحديد واستعراض بعض المفاهيم ذات العلاقة والمدلول بالجريمة ذاتها، وذلك على النحو الآتي:

١. الجريمة في اللغة:

الجريمة هي الفعل الذي يستوجب عقاباً. ويوجب ملاماً. أصل كلمة جريمة من جرم بمعنى كسب وقطع، والجرم الذنب. وهي الكسب المكروه غير المستحسن وجرم يراد منها الحمل على فعل حملاً آثماً(٨). قال الله سبحانه وتعالى: (وَيَا قَوْمِ لَا يَجْرِمَنَّكُمْ شِقَاقِي أَنْ يُصِيبَكُمْ مِثْلُ مَا أَصَابَ قَوْمَ نُوحٍ أَوْ قَوْمَ هُودٍ أَوْ قَوْمَ صَالِحٍ وَمَا قَوْمُ لُوطٍ مِنْكُمْ بِبَعِيدٍ (٨٩) وَاسْتَغْفِرُوا رَبَّكُمْ ثُمَّ تُوبُوا إِلَيْهِ إِنَّ رَبِّي رَحِيمٌ وَدُودٌ)(٩). وقال جلّ جلاله: (وَلَا يَجْرِمَنَّكُمْ شَنَآنُ قَوْمٍ عَلَى أَلَّا تَعْدِلُوا اعْدِلُوا هُوَ أَقْرَبُ لِلتَّقْوَى وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ خَبِيرٌ بِمَا تَعْمَلُونَ) (١٠).

٢. الجريمة في الاصطلاح الفقهي:

قيل: إن الجريمة هي فعل ما نهى عنه الله وعصيان ما أمر به. وعرفت الجريمة في هذا المجال: بأنها إتيان فعل محرم معاقب على فعله، أو ترك فعل مأمور به معاقب على تركه؛ وذلك لأن الله قرّر عقاباً لكل من يخالف أوامره ونواهيه وهو إمّا يكون عقاباً في الدنيا ينفذه الحاكم، وإمّا أن يكون تكليفاً يكفى به عما ارتكب في جنب الله، وإما أن يكون عقاباً في الآخرة (١١).

٣. الجريمة في القانون الوضعي:

تعرف الجريمة بأنها الفعل الذي يقع بالمخالفة لقانون العقوبات. أو أنها فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدابير احترازياً. وهناك من يريد التعريف السابق تفصيلاً، حيث الجريمة هي كل عمل أو امتناع يجرمه النظام القانوني، ويقرر له جزاءً جنائياً هو العقوبة، توقعه الدولة عن طريق الإجراءات التي رسمها المشروع. وتعرف الجريمة بأنها " سلوك إنساني معاقب عليه بوصفه خرقاً أو تهديداً لقيم المجتمع أو لمصالح أفراده الأساسية، أو لما يعتبره المشرع كذلك، ووسيلته في ذلك النص الجنائي"(١٢).

٤. المفهوم الاجتماعي للجريمة:

يرتكز هذا المفهوم على أساس الربط بين الجريمة وبين مصالح وقيم المجتمع، ويرى أصحاب هذا المفهوم بأن الجريمة تقتضي وجود قيم معينة تحظى باهتمام وقبول لدى الدولة، الأمر الذي يتطلب حمايتها وتحريم كل فعل من شأنه المساس بها. وقد يسلك بعض الأفراد في المجتمع مسلكاً ضاراً بهذه القيم فيترتب على مسلكهم هذا حدوث ردود فعل من قبل السلطة المختصة بحماية تلك القيم تتمثل في إجراءات ووسائل إكراه وإجبار يتم إنزالها بمرتكبي هذه الأفعال. وقد طرح أنصار هذا الاتجاه تعريفات عدة للجريمة، نبدأها بتعريف لدور الجريمة مفاده: أن الجريمة هي كل فعل أو امتناع يتعارض مع القيم والأفكار التي استقرت في وجدان الجماعة. وقال آخرون: بأنها كل فعل يقدم الشخص على ارتكابه بدوافع فردية خالصة تقلق حياة الجماعة وتتعارض مع المستوى الخلقي السائد لديها في لحظة معينة من الزمن.

٥. المفهوم الأخلاقي للجريمة:

الأخلاق لدى جماعة أو أمة هي مجموع ما يدين به أفرادها من مبادئ ومُثل وقيم سامية يقدسونها ويحرمون الخروج عليها.

٦. المفهوم الطبيعي للجريمة:

يقول أنصار هذا المفهوم: أن هناك طائفة من الأفعال التي اعتبرت جريمة في كافة الأزمنة والأماكن، وذلك أنها تتعارض مع المشاعر الأدبية التي نبتت في المجتمع وتطورت بتطوره وانتقلت من جيل إلى جيل عن طريق التقليد والوراثة (١٣).

٧. **الجريمة:**

هي (سلوك ينتهك القواعد الأخلاقية التي وضعت لها الجماعة جزاءات سلبية تحمل صفة الرسمية)، أو هي: (السلوك الذي تحرمه الدولة لما يترتب عليه من ضرر على المجتمع، والذي تتدخل لمنعه بعقاب مرتكبيه).

٨. **المجرم:**

هو الفرد الذي ينتهك القوانين والقواعد الجنائية في مجتمع ما مع سبق الإصرار، أو هو الشخص الذي يرتكب فعلاً غير اجتماعي سواء كان بقصد ارتكاب جريمة أم لا. ويشمل هذا المعنى كل من ينتهك أو يتصرف على نحو يخالف المعايير الاجتماعية.

٩. **السلوك الإجرامي:**

هو أي سلوك مضاد للمجتمع، وموجه ضد المصلحة العامة، أو هو أي شكل من أشكال مخالفة المعايير الأخلاقية التي يرتضيها مجتمع معين، ويعاقب عليها القانون. وباختصار إذا كانت الجريمة هي مسمى الفعل الإجرامي، فإن السلوك الإجرامي هو ممارسة هذا الفعل.

١٠. **الانحراف:**

ويقصد به عدم مسايرة أو مجارات المعايير الاجتماعية السائدة في المجتمع، أو هو الابتعاد أو الاختلاف عن خط معين أو معيار محكي.

١١. **الجنوح:**

أية انتهاكات للقانون يقوم بها الأشخاص الصغار أو الأحداث وتعد أقل خطورة (١٤).

٣- تصنيف المجرمين :

نتيجة لتطور المجتمعات وتقدمها، تنوعت وتعددت المفاهيم والتصانيف المتعلقة بتقسيم وتصنيف المجرمين، وظهرت العديد من النظريات والتي يقف خلفها العديد من المهتمين بشؤون المجتمعات من رجال وعلماء القانون وعلم النفس وعلماء الاجتماع... الخ، ولقد ظهرت تصنيفات عدة للمجرمين منها:

أولاً: التصنيف القانوني للمجرمين.

يُعد التصنيف القانوني للجريمة والمجرمين أقدم التصنيفات وأهمها، ويتحدد هذا التصنيف على أساس أن يطلق عنوان الجرم على ما قام به وصنف بمقتضاه، فالقاتل هو المتهم في جريمة قتل

أو المحكوم عليه بها. ثم ظهرت بعد ذلك التفرقة بين الجريمة على أساس جسامة السلوك إلى مخالفات وجنح وجنايات. ووضعت التصنيفات القانونية طبقاً للموضوع الذي يتجه إليه السلوك الإجرامي. فهناك جرائم ضد الأشخاص، وأخرى ضد الأموال، وهناك جرائم عامة، وجرائم سياسية. وبعد ذلك قدمت تصنيفات عديدة منها تصنيف "جاروفالو" إذ وضع " جاروفالو" تصنيفاً رباعياً لأنماط المجرمين يمتزج فيه تفكيره الوضعي في نشأة الجريمة مع اتجاهه القانوني، وذلك على النحو الآتي:

أ- المجرم القاتل:

نظر إليه (جاروفالو) على أنه يمثل النمط الشائع للمجرمين، فهو أناني يفتقر إلى روح الإيثار، وهو خلو من عواطف الرحمة والعدل، وهذا الصنف من المجرمين قادر على أن يرتكب أي نوع من أنواع السلوك الإجرامي، فهو يقتل ويسرق ويتخلص من زوجته حتى يتسنى له الزواج بأخرى وهكذا.

ب- المجرم العنيف:

يصنف إلى نوعين: الأول/ هو المجرم الانفعالي، وهو الذي تثيره الخمور أو أية ظروف انفعالية غير عادية، أما النوع الثاني/ فهو الذي يرتكب الجرائم المتوطنة كجرائم الأخذ بالثأر في بعض المناطق. أو يقدم على الاغتيالات السياسية في مناطق أخرى وفي أزمنة محدودة.

ج- المجرم غير الأمين:

وهو الذي يفتقر إلى الأمانة والنزاهة ويرتكب معظم جرائمه ضد الملكيات.

د- المجرم الفاسد جنسياً:

وهو الذي يتجه سلوكه الإجرامي ضد العفة والطهارة الجنسية ويمارس العديد من الجرائم الجنسية.

ثانياً: التصنيف البيولوجي للمجرمين:

هو التصنيف الذي تمّ في ضوء تأكيد المحددات البيولوجية والوراثية وقد صنف "لمبروزو" المجرمين إلى ثلاثة أنواع وذلك على النحو الآتي:

١- **المجرمون بالفطرة:**

هم الذين يرثون عن آبائهم مجموعة من الخصائص الجسمية والعقلية التي تؤدي إلى الانحراف الإجرامي، وهؤلاء يشكلون حوالي ثلث عدد المجرمين في المجتمع.

٢- **المجرمون نتيجة المرض:**

هم الذين يعانون من بعض الأمراض أو الاضطرابات النفسية والعقلية أو العضوية مثل الصرع والهستريا وغيرها مما يمثل السبب الأساسي في إقدام هؤلاء الأفراد على الجريمة.

٣- **أشباه المجرمين:**

يكون هؤلاء عادة أصحاء الجسم ولا يعانون من نقص عقل، ولكنهم يتسمون بحالة عقلية لا تؤهلهم لأن يسلكون مسلكاً طبيعياً في بعض المواقف التي يتعرضون لها.

ثالثاً: التصنيف النفسي للمجرمين:

هو التصنيف الذي يضع في الاعتبار فهم شخصية المجرم وخصاله النفسية والانفعالية ودوافعه اللاشعورية، وكافة الاضطرابات النفسية والعقلية التي يمكن أن يعاني منها المجرم، وكذلك صراعاته النفسية وغير ذلك، وفيما يلي عرض لواحد من أهم التصنيفات النفسية وهو تصنيف (كورزيني) حيث صنّف المجرمين إلى سبع فئات هي على النحو الآتي:

١- المجرم العرضي، مثل السائق الطائش الذي يرتكب الجريمة دون أن يقصدها.

٢- المجرم الموقفي، وهو الذي يبرر مشروعية جريمته بظروف محددة، مثل الذي يسرق رغيف الخبز ليتفادى الموت جوعاً.

٣- المجرم غير المسؤول كالطفل والمعتوه.

٤- المجرم العصابي، وهو الذي يرتكب جريمته؛ لأن لديه مشكلة يريد أن يواجهها ويقضي عليها رغم أنه لا يدرك ما يواجهه، ولا يدرك كذلك أنه يواجه أمراً ما.

٥- المجرم السيكوباتي.

٦- المجرم غير المتزن انفعالياً كالذي يستخدم العنف في ارتكاب الجرائم الجنسية.

٧- المجرم المحترف، وهو الذي يكسب عيشه عن طريق احتراف السلوك الإجرامي.

رابعاً: التصنيف الاجتماعي للمجرمين:

هو التصنيف الذي يتم في ضوء تحديد القوى الاجتماعية التي تؤدي إلى خلق المجرمين في ضوء ثقافة خاصة تسمو على العوامل الفردية، فقد تكون الجريمة لدى بعض المجرمين أسلوباً للحياة وطريقاً لكسب العيش، وينظم المجرم حياته في ظل نظرته إليها على أنها مهنة وحرفة وعمل. وفي ضوء هذه النظرة يتشكل عالم الجريمة في مستويات يحددها بناء المجتمع وثقافته. وتظهر هذه المستويات في تفاوت أسلوب حياة الإنسان المجرم. وذلك على النحو الآتي:

١- أسلوب حياة المجرم العادي:

يضم هذا الأسلوب الإجرامي أغلب المجرمين الذين يكسبون عيشهم بارتكابهم الجرائم التقليدية ضد الممتلكات. وينشأ أغلب أعضاء هذه الفئة في أسر فقيرة ويعيشون في أحياء شعبية ينقصها الكثير من الخدمات واهتمام المسؤولين. ويتميز المجرم العادي عن فئتين من المجرمين الآخرين. الأولى: فئة المجرمين الذين يأتي إجرامهم عرضياً كمدمني الخمور والمخدرات وغير المتخصصين من الخارجين على القانون، وهؤلاء لا يتخذون من الجريمة وسيلة للعيش. أما الفئة الثانية فيأتي أفرادها في مرتبة أعلى من الإجرام وهم محترفوا الإجرام ممن سنتحدث عنهم في الفقرة الآتية:

٣- أسلوب حياة المجرم المحترف:

يختلف المجرم المحترف عن المجرم العادي في اعتبارات عديدة منها أنه يستخدم وسائل في أسلوبه الإجرامي أكثر تعقيداً وكفاية وفاعلية لتنفيذ جرائمه. وللمجرم المحترف نشاط واسع ومتعدد الجوانب، وله من الناس من يساندونه أكثر من المجرم العادي، ويشعر بانتمائه الطبقي إلى فئة معينة. فالمجرمون المحترفون يدركون مهارتهم الفنية الخاصة نحو المجرمين والهواة ممن يرتكبون الجريمة بأسلوب فج وينظرون إلى الهواة نظرة محتقرة، ويتجنبون الاختلاط بهم ورفقتهم والتوحد معهم. فالمجرم المحترف حاذق يستطيع أن يتقن عمله بصورة عادية. فمن بين المجرمين العاديين من يقوم بالسرقة، ولكن المحترف يقوم بها في صورة غير عادية وبمهارة كبيرة يستطيع بها أن يحصل على أكبر قدر من المال دون أن يتعرض للقبض عليه. ولذا فالمحترف أقل استخداماً للعنف وأكثر استخداماً للعقل من المجرم العادي. لذلك يندرج في فئة المجرمين المحترفين: النشال وسارق المتاجر والبنوك ومحلات المجوهرات ومزور الشيكات ومزيف النقود. هذا بالإضافة إلى أشكال أخرى من السلوك الإجرامي يمكن أن يقوم بها المجرم المحترف مثل الابتزاز وتزييف اللوحات الفنية والغش في ألعاب القمار.. الخ.

٣- أسلوب حياة المجرم المنظم.

هو المجرم الذي يعمل في إطار جماعة إجرامية منظمة، تختلف معايير تنظيمها عن المعايير المنظمة لأسلوبي الجريمة العادية والاحتراف. فالرابطة التي تجمع المجرمين العاديين والمحترفين رابطة إرادية تتحدد طوعاً وبرغبة المجرم، وهي رابطة أساسها التعاون، وخالية من كل تدرج وتسلسل في المرتبة الإجتماعية. وإذا كان في هذه الرابطة تخطيط مشترك يسهم فيه كل فرد فإن هناك حداً أدنى من التوجيه والإشراف بها. أما الجريمة المنظمة فأساس تنظيمها تركيز الزعامة والتدرج في المراكز الاجتماعية والإدراة المعقدة والضوابط الاجتماعية المنوّعة وتعدد مجالات العمل الإجرامي وتقسيمه والتخصص فيه. ويتركز نشاط المجرمين المنظمين في عرض وتوزيع السلع والخدمات التي يحرمها القانون. ويتحدد استمرار الجريمة المنظمة في المجتمع بناء على استمرار حاجة المجتمع إلى هذه السلع والخدمات غير المشروعة والمزدولة. ويتمثل نشاط هؤلاء المجرمين في القمار والدعارة والمخدرات والتهريب وطبع ونشر المطبوعات المحرمة قانوناً. كما اتسعت في السنوات الأخيرة مجالات الجريمة المنظمة لتغزو مجالات الصناعة والعمل والخدمات الترويحية.

السمة المميزة لهذا النوع من النشاط الإجرامي أنه يتعامل مع عملاء وليس ضحايا كما في أسلوب المجرم العادي والمجرم المحترف. إذ لا يوجد ما يجبر الفرد على أن يتعامل مع تنظيم للدعارة أو للبضائع المهربة أو للقمار، بل يسعى الفرد إلى الحصول على هذه الخدمات بإرادته ويدفع مقابل ما يأخذه من سلع أو ما يحصل عليه من خدمة. لذلك فإن أسلوب التنظيم الإجرامي مع عملائه يخلو – غالباً – من طابع العنف. أما مظاهر العنف التي ترتبط بالجريمة المنظمة فإنها تتجه أساساً إلى الأطراف الذين يقعون في صراع مع التنظيم الإجرامي، سواء من داخله أو خارجه.

خامساً: تصنيف المجرمين في ضوء المنحنى التكاملي:

حاول أصحاب التفسير التكاملي للجريمة أو اتجاه العوامل المتعددة وضع تنميط أو تصنيف إجرامي يتفق مع تصورهم النظري للتوفيق بين التفسيرات البيولوجية والنفسية والاجتماعية. وهناك محاولات عديدة للتصنيف في ضوء هذا التفسير التكاملي، وتأتي محاولة تصنيف "فون ليست" في مقدمة تلك المحاولات، وكانت وفق الشكل الآتي:

١- حالات إجرامية يفتقر فيها المجرم إلى الوعي الكامل أو يلابس وعيه الغموض بأنه أضر بحقوق الآخرين. وهنا يظهر المنشأ النفسي للجريمة في حالات الطيش أو الجهل أو الإهمال.

٢- حالات إجرامية يرتبط فيها المجرم بغيره ارتباطاً عاطفياً أو يكن له حباً وولاءً، ويدفع ذلك الارتباط العاطفي إلى ارتكاب الجريمة من أجل من يرتبط به ويحبه.

٣- حالات إجرامية يؤدي فيها دافع المحافظة على النفس إلى الجريمة، كما في حالات جرائم العوز الاقتصادي والجرائم الناجمة عن الخوف من العقاب أو الفضيحة أو العار.

٤- حالات الجرائم الجنسية.

٥- حالات الجرائم الانفعالية، كالجرائم التي يرتكبها شخص نتيجة لتعرضه لإهانة معينة، أو عندما يرتكب شخص آخر جريمة ضد شخص ثان رفض حبه، أو جرائم الرغبة في الانتقام، أو الغيرة، أو الكراهية، أو الغضب، أو الحسد.

٦- حالات إجرامية دافعها الرغبة في المجد والشهرة.

٧- حالات إجرامية دافعها الكسب السريع والجشع، يتفرع من هذا النوع من حالات احتراف الجريمة سعياً وراء لذة، أو إعراضاً عن العمل وكرهاً فيه.

أما التصنيف الآخر في هذا المجال، هو تصنيف "كلينارد وكويني". إذ استند الباحثان في محاولة تصنيفهما للمجرمين إلى أربع خصائص هي مسار السلوك الإجرامي خلال تاريخ حياة المجرم، ومدى التأييد والعون الذي يلقاه المجرم من جانب جماعة ما نظير إقدامه على ارتكاب السلوك الإجرامي، واستجابة المجتمع أو رد فعله إزاء السلوك الإجرامي، والتناظر بين أنماط السلوك الإجرامي وأنماط السلوك المشروع. وفي ضوء هذه الخصائص صنّف الباحثان المجرمين إلى الفئات الآتية:

١- مجرمون يتسم إجرامهم بالعنف نحو الأشخاص كالقتلة والمغتصبين بالقوة.

٢- مجرمون يتسم إجرامهم بالطابع العارض ويوجه إجرامهم ضد الممتلكات كسارقي السيارات ولصوص المتاجر ومزوري الشيكات والمخربين.

٣- مجرمو المهنة، ويبدو سلوكهم الإجرامي خلال أدائهم للمهنة التي يعملون بها في الاختلاس والغش والتخريب والتجسس... الخ.

٤- مجرمون يتجه سلوكهم الإجرامي ضد النظام كمدمني الخمور ومتعاطي المخدرات والتشرد والدعارة واللواط.... إلخ.

٥- مجرمون سياسيون، يظهر سلوكهم الإجرامي في جرائم الخيانة العظمى والعصيان والتمرد وإثارة الفتن والشغب والتخريب والتجسس.

٦- المجرمون التقليديون، وهم الذين يرتكبون جرائم السطو والسرقة.

٧- المجرمون الذين يرتكبون الجرائم المنظمة، كالبلطجة وتجارة الدعارة والقمار والتجارة في المخدرات.

٨- المجرمون المحترفون، كسارق المتاجر والنشال والمزّيف... إلخ (١٥).

مهما تعددت التصنيفات الخاصة بالمجرمين وتنوعت، فإن ظاهرة الجريمة والمجرمين، ما زالت موضع اهتمام علماء القانون والاجتماع وعلم النفس؛ لما تتركه من أثر سلبي في العلاقات الإنسانية وإهدار القيم والعادات والتقاليد السائدة في المجتمع، وتنال من إنسانية الإنسان. ويلاحظ مما سبق: أن تلك التصنيفات لم تتطرق إلى المجرم الحديث (المجرم الإلكتروني) الذي يرتكب جرائمه من خلال تكنولوجيا المعلومات.

٤- تصنيف الجرائم.

مثلما صنّف المهتمون بشؤون المجتمعات من علماء ومفكرين وباحثين مختلفين، صنّف هؤلاء الجرائم كذلك، وذلك من أجل الوقوف على ماهيّة كل صنف من تلك الأصناف في محاولة لوضع أسس وترسيخ العدالة في المجتمع الإنساني. في أحيان عديدة يرتبط تصنيف المجرمين بالأطر أو المناحي النظرية المفسرة للسلوك الإجرامي. أما تصنيف الجرائم فهو أقرب إلى اتباع القانون الجنائي بشكل أساسي. لذلك فهناك تصنيفات عديدة للجرائم حسب دوافع ارتكابها أو مكان ارتكابها أو مترتباتها وآثارها. وتقسم الجرائم في المجتمع وفق عدد من المحطات الرئيسة.

في ضوء ما سبق قد يكون من الممكن إجراء العديد من التقسيمات استناداً إلى معايير متنوعة؛ كمعيار المصلحة الإجتماعية محل العدوان في الجريمة، ومعيار طرق تنفيذ الجريمة، بل إن مظاهر الإجرام الحديث الناشئ عن تجريم المشرع لبعض الأفعال التي تشكل اعتداء على قيم أو مصالح جديدة توحي هي الأخرى بتقسيمات متنوعة. وعلى أية حال نكتفي في هذا المقام بالتعرض - بإيجاز- لتقسيم الجرائم حسب الباعث الإجرامي، وتقسيمها بحسب عدد القائمين على المشروع الإجرامي، ومن ثم سنعرض للجرائم وما المقصود بها من ناحية القانون الجنائي على وجه التحديد.

وفيما يلي نعرض للتصنيفات التي حددّت أو قسّمت في ضوئها الجرائم وبالشكل الآتي:

أولاً: تقسيم الجرائم بحسب الباعث الإجرامي:

وفي ضوء هذا التصنيف تقسم الجرائم وفق الشكل الآتي:

١- جرائم العنف:

وهي طائفة الجرائم التي تتسم بردود الفعل البدائية من جانب الجاني، وتنطوي على قدر من العنف يتفاوت في مقداره. ولهذا يطلق عليها اسم (Lecvime primitif). وترتبط هذه التسمية بطائفة المجرمين ذوي رد الفعل البدائي، وهي طائفة من المجرمين في عالم الإجرام سيلج بدراستهم وتحليل سلوكهم.

تنشأ هذه الطائفة من جرائم العنف نتيجة إندلاع فُجائي للنشاط الإجرامي لدى الشخص دون أن يملك القدرة على السيطرة على هذا الاندلاع. ومثال ذلك: جريمة القتل التي تقع من الشخص في حالة تفجر غضبه.

تغطي ردود الفعل البدائية للشخص في هذه الحالة صورتين مختلفتين: الأولى/ ردود الفعل المتفجرة المرتبطة إما بصورة غضب فجائي تنتاب الشخص، وإما بتراكم عاطفي لغضبه على نحو يثير رد فعله الزائد عن الحد بسبب أي حادث بسيط يتعرض له (كالمجرم الذي يقتل أفراد أسرته نتيجة للحقد المتراكم لديه إزاءهم). وتصدر ردود الفعل هذه غالباً عن أشخاص يعتريهم الاهتياج الشديد أو الصراع.

الثانية/ الأفعال العنيفة المتقطعة التي تصدر فجأة دون مقدمات عن أشخاص مصابين بمرض عقلي. ولفقد الشخص سيطرته على حالة العنف التي تعتريه فإنه يعجز عن ضبط ردود فعله أو اتخاذ مسلك يتناسب مع الموقف الذي يتعرض له (كمن يسرقن فجأة بعض الحاجيات أثناء تواجدهن في المحلات الكبيرة). ويتعذر في هذه الحالة الوقوف على الباعث على ارتكاب الجريمة.

٢- الجرائم النفعية:

يلجأ الشخص لارتكاب هذه الجرائم لهدف نفعي محض كأن يجد في هذه الجرمية حلاً يتخلص به من مأزق أو مشكلة يتعرض لها؛ ومثال ذلك: الزوجة التي تقتل زوجها لكي تتخلص من سوء معاملته لها؛ أو الشخص الذي يحرق المال المُؤَمّن عليه لكي يتيسر له الحصول على مبلغ التأمين، وكذلك الصراف الذي يسرق بغية الحصول على المال اللازم لإشباع نزواته.

للجريمة النفعية على النحو السابق تعريفه أربع خصائص:

١- إنها تفترض تعرض المجرم لموقف خاص أو يمثل لديه خطورة.

٢- إنها قاصرة على شكل واحد من أشكال الجرائم أو موجهه إلى شخص واحد أو لمجموعة بعينها من الأشخاص.

٣- إنها تعد نتيجة لأزمة يعاني منها الشخص كضرورة إذعانه لأمر ما.

٤- إنها تنتشر في مجال جرائم الأموال (كاختلاس الموظف للمال)، وكذلك في مجال جرائم الاعتداء على الأشخاص (كالقتل بهدف الاستيلاء على ثروة المجني عليه، أو قتل الزوجة لزوجها لكي يخلو لها الجو مع عشيقها).

٣- جرائم إرساء العدالة الكاذبة:

الفكرة الجوهرية في هذه الطائفة من الجرائم: أن المجرم فيها إنما يرتكب الفعل اعتقاداً منه بصحة ما يقوم به، بل وبأنه من الواجب عليه القيام بذلك. وعلى العكس من طائفة الجرائم النفعية التي يهدف من ورائها المجرم إلى تحقيق مصلحة أنانية بحتة، فإن المجرم في هذه الطائفة التي نحن بصددها يعتقد بعدالة ما يقوم به سواء كان ذلك في مجال العلاقات مع غيره من الأفراد، أو فيما يخص العلاقة مع الدولة.

تغطي جريمة إرساء العدالة الكاذبة صوراً متنوعة كجريمة القتل العاطفي، والجريمة المذهبية أو السياسية دفاعاً عن عقيدة دينية أو مبدأ فكرة سياسية، وكالقتل إشفاقاً، وهو قتل المريض بمرض لا يرجس الشفاء منه اعتقاداً من الجاني بأنه بهذا السلوك إنما يخلص المجنى عليه من آلامه، ومثالها الجريمة التي يرتكبها الشخص بهدف إسداء خدمة إلى شخص آخر يعتقد بعدالة قضيته، كمن يقتل صاحب المنزل لكي يخلص خادمته من سوء التعذيب الذي تتعرض له على يد مخدومها.

٤- الجرائم المنظمة:

تتمثل في الجريمة التي تكشف عن إرادة واعية لارتكاب فعل أو عدة أفعال إجرامية. ومثال ذلك جرائم السطو، وجرائم النشل والسرقة داخل الفنادق، وجرائم النصب. ويتطلب هذا النوع من الجرائم إعداداً خاصاً يبدأ من البحث على مناسبة لارتكاب الجريمة، وإعداد خطة التنفيذ، والتعرف على مكان ارتكاب الجريمة، والأدوات اللازمة لذلك، واختيار الشركاء.

ويمكن التمييز في مجال الجرائم المنظمة بين ثلاثة أشكال مختلفة:

١- الجرائم المنظمة ذات الطابع الوحشي أو العنيف كالسطو المسلح والسرقة بإكراه والنشل.

٢- الجرائم التي تتمثل في نشاط غير مشروع بهدف الربح، كالقوادة والاتجار في المخدرات.

٣- الجرائم المسماة بجرائم الياقات البيضاء والتي يرتكبها أشخاص ينتمون إلى طبقات اجتماعية عليا وتعتمد على الدهاء في ارتكابها كالتهرب من الضرائب وكجرائم الشركات في المجال الاقتصادي ورشوة الموظفين (١٦).

ثانياً: تقسيم الجرائم وفقاً لعدد القائمين على المشروع الإجرامي.

يتم تقسيم الجرائم وفق هذا المقياس بالشكل الآتي:

١- ضابط هذا التقسيم:

تقوم فكرة هذا التقسيم على عدد الأفراد الذين يضطلعون بدور في إتمام المشروع الإجرامي. إذ من الثابت أن الجريمة تختلف من حيث طبيعتها، ومن حيث بنائها القانوني، ومن حيث كيفية تنفيذها بحسب عدد الأفراد الذين يشتركون فيها. ومن هذه الزاوية يمكن تقسيم الجرائم إلى أنواع ثلاثة:

أولاً: جرائم الفرد الواحد:

يقصد بهذه الطائفة كافة الجرائم التي يضطلع فرد واحد بالتفكير فيها والإعداد لها، وكذلك تنفيذها. وبالنظر إلى أن المجرم الواحد يكون محدوداً عادة من حيث إمكاناته المادية والذهنية، فإن نشاطه يقتصر بالضرورة على ارتكاب نماذج معينة من الجرائم وعلى استعمال طرق معينة لتنفيذها. وباعتماد هذا الشخص على مهارته فإنه يحاول تعويض النقص الناشئ عن عدم وجود آخرين معه. وتتنوع جرائم الفرد الواحد تنوعاً كبيراً، ومن أمثلتها: جرائم القتل العاطفي والسرقة بالاحتراف.

ثانياً: جرائم الاشتراك:

تشمل هذه النوعية من الجرائم كافة الحالات التي يعاقب فيها القانون الجنائي على اشتراك أكثر من شخص في ارتكاب الجريمة سواء في صورة الجرائم التي يرتكبها فاعل مع غيره، أو تلك التي يشترك فيها مع الفاعل الأصلي مساهمين.

لا شك أن كافة صور الاشتراك في الجريمة من جانب عدة أشخاص لها أهميتها الخاصة من الناحية القانونية. فالمشرع يعاقب - كقاعدة عامة - الشريك بالعقوبة المقررة للفاعل الأصلي. وليس ذلك إلا نتيجة للدور الخطير الذي يقوم به الشريك، والذي قد لا يقل في حقيقة الأمر عن الدور الذي يحتجزه الفاعل الأصلي لنفسه. والاشتراك في الجريمة قد يتم بالتحريض أو بالاتفاق أو المساعدة.

مع ذلك، فإن جرائم الاشتراك - من منظورها الإجرامي - لا تقتصر فقط على صور المساهمة الجنائية التقليدية السابق ذكرها، وإنما تشمل صوراً أخرى ليست أقل أهمية مثل إخفاء الأشياء المتحصلة من جريمة؛ فالجريمة هنا تقع من طرفين: مجرم الفعل الأصلي (كالسرقة)، والمجرم الذي أخفى الأشياء المسروقة. وتجدر الإشارة إلى أن جريمة الإخفاء تعتبر ومنذ سنة (١٩٠٤) جريمة مستقلة، وقائمة بذاتها عن الجريمة الأصلية. أما قبل هذا التاريخ فكانت تعد صورة من صور المساهمة الجنائية. كما تشمل جرائم الإشتراك - بخلاف صور المساهمة الجنائية التقليدية - الجريمة التي يقوم على ارتكابها الفاعل الأصلي ومن يحركه أو يحثه على ذلك حين لا يكون ممكناً اعتبار هذا الشخص الأخير مساهماً بالتحريض. وبالتالي يمكن أن نرى في جرائم الإشتراك صورتين من المساهمة: الأولى/ بالتعويض، والثانية/ بالإغراء أو بالنصيحة.

ثالثاً: جرائم التجمعات:

يقصد بها الفعل الإجرامي أو مجموعة الأفعال الإجرامية التي يرتكبها حشد من الأفراد المتجمعين سواء كان ذلك بصورة تلقائية أو بناء على طلب أو إيحاء من متزعمي التجمهر.

تتميز هذه الطائفة من الجرائم بخصيصتين أساسيتين هما:

الأولى: الدور الذي يقوم به متزعمو التجمهر في الإيحاء للجمهور بارتكاب الفعل الإجرامي وكذلك الإعداد. ويختلف هذا الدور بحسب الأحوال، فقد يتمثل في قرار استخدام المظاهرة أو الحشد كوسيلة لارتكاب أفعال غير مشروعة وذلك بهدف إثارة رد الفعل العنيف من جانب قوات البوليس. وقد يأخذ هذا الدور على العكس صورة تنظيم مجموعة لحفظ النظام للحيلولة دون حدوث الفوضى التي تقع من جانب الجمهور.

الثانية: طبيعة الظاهرة النفسية والاجتماعية التي تؤدي أحياناً إلى وقوع الجريمة من جانب أشخاص منفردين ليسوا بحسب الأصل مجرمين، لكنهم لا يتورعون عن الانخراط في هذا المسلك الإجرامي منتهزين فرصة تواجدهم بين المتجمهرين، ويفسر البعض مسلك

هؤلاء الأشخاص بتأثير الإيحاء الجماعي الذي يمارسه الجمهور عليهم، أو بالنظر إليه على أنه من قبيل الجريمة العاطفية، والأرجح - كما يرى البعض الآخر - أن التجمهر يوقظ داخل هؤلاء الأفراد - الذين هم بحسب الأصل غير مجرمين - بعض النزعات العميقة الإجرامية (١٧).

ثالثاً: تقسيم أو تصنيف الجرائم حسب القانون الجنائي:

صنّف القانون الجنائي الجرائم وفق الشكل الآتي:

أولاً: جرائم المخدرات والكحوليات:

تُعرف جرائم المخدرات بأنها الجرائم التي يقوم مرتكبوها باستخدام المواد المخدرة أو إنتاجها أو تهريبها وترويجها. أو هي بمعنى آخر: (تلك الجرائم التي تشتمل على إنتاج المواد المخدرة وتهريبها وترويجها وحيازتها واستعمالها، ويدخل في ذلك العقاقير المخدرة الممنوع استعمالها إلا بوصفة طبية).

يلزم لوقوع هذه الجرائم توافر ثلاثة أركان أساسية هي:

١- الفعل المادي: أي الاتصال غير المشروع بالمواد المخدرة المحظورة.

٢- المادة المخدرة المحظورة: أي لا بد لوقوع جريمة المخدرات أن يكون الفعل متصلاً بإحدى المواد التي حدّدها نظام المخدرات وحظر التعامل معها.

٣- القصد الجنائي: وهو الركن المعنوي للجريمة، ويكفي لتوافره علم الشخص بوجود المادة المخدرة لديه أو أن تكون إرادته في وجودها لديه حرة طليقة.

تقترن جرائم المخدرات بتفاقم السلوك الإجرامي مما يهدد سلامة المجتمع وأمنه، حيث لوحظ أن أغلب جرائم العنف والسرقة والخطف والاغتصاب والقتل يرتكبها متعاطو المواد المخدرة، إما نتيجة للاضطراب النفسي والعقلي الذي تحدثه تلك المواد أو رغبة في تدبير الأموال اللأزمة للحصول على المخدرات.

وفيما يلي عرض موجز لأهم جرائم المخدرات:

١- إنتاج المخدرات:

وهو نوع أساسي من جرائم المخدرات، رغم أن كثيراً من الباحثين لا يشير إليه عند تعريفه لهذه الفئة من الجرائم. ويشمل إنتاج المخدرات أساليب عديدة منها جمعها من النباتات البرية.

وهناك مخدرات تجمع أو تصنع من نباتات تزرع خاصة لهذا الغرض مثل القنب الهندي، والخشاش الذي يستخرج منه الأفيون الذي يعد من المخدرات الأساسية.

٢- تهريب المخدرات:

يشمل هذا النوع من جرائم المخدرات عمليات تهريبها والاتجار فيها بطريقة بالغة الدقة يقوم بها أصحاب مزارع المخدرات مع كبار التجار والمهربين، ويستغلون بعض الأشخاص الذين يقومون بنقل المخدرات من مراكز الإنتاج أو التجميع أو التغليف إلى مناطق التسويق. وهذه العملية من أخطرها على الإطلاق. ويستخدم في تنفيذها إمكانات بشرية مسلحة بالمال والعتاد، وتحتاج إلى خبرة وحيلة واسعتين.

وتستخدم كافة الأساليب والإمكانات المتاحة لإخفاء المخدرات للتهرب من الشرطة. وكل يوم يبتكر مهربو ومروجو المخدرات حيلاً وطرقاً إجرامية جديدة.

أما فيما يتعلق بتوزيع المخدرات على متعاطيها في عبوات صغيرة، فيعتمد التجار عادة على مدمني المخدرات الذين يقومون بهذا العمل الإجرامي من أجل حصولهم هم أنفسهم على حاجتهم منها دون تكبد أية نفقات.

٣- تعاطي المخدرات:

يتمثل هذا النوع من الجرائم في تعاطي الشخص بنفسه أي نوع من أنواع المخدرات المحظورة قانوناً، والتي يترتب عليها أضرار شديدة الوطأة على المتعاطي نفسه وعلى أقرانه. ويسمي بعض الباحثين جرائم تعاطي المخدرات بالجرائم العامة، وأحياناً الجرائم المستمرة.

ثانياً: الجرائم الجنسية:

هناك تعريفات عديدة لمفهوم الجريمة الجنسية، منها أنه أي سلوك جنسي يجرمه التشريع القائم ويعاقب عليه. أو هي أي فعل أو سلوك يرتكب ضد أخلاق الجنس في مجتمع معين ويعاقب عليه القانون القائم. لذلك فإننا نتوقع وجود فروق حضارية وثقافية واضحة بين المجتمعات فيما يجرمه التشريع من أشكال السلوك الجنسي.

يمكن تصنيف الجرائم الجنسية إلى فئتين أساسيتين هما:

١- الجرائم الجنسية الغيرية:

وهي أي سلوك جنسي يجرمه التشريع القائم في المجتمع ويعاقب عليه، ويكون السلوك الإجرامي موجهاً إلى الأشخاص من الجنس الآخر، سواء كانوا رجالاً أم نساء. ومن هذه الجرائم ما يلي:

أ- البغاء:

يعرف بأنه إباحة المرأة نفسها لارتكاب الفحشاء مع الناس بدون تمييز نظير أجر تحصل عليه.

ب- الاغتصاب:

ويعرف بأنه الاتصال الجنسي بامرأة ضد إرادتها بالقوة أو بأي شكل من أشكال التهديد.

ج- الزنا:

يقصد به الجماع أو العلاقة الجنسية غير الشرعية بين رجل وامرأة يكون أحدهما متزوجاً، أو بمعنى آخر وجود شريك يجامع الزوجة أو شريكة تجامع الزوج جماعاً غير شرعي.

د- هتك العرض:

وهو التعدي الفاحش المنافي للآداب الذي يقع على جسم أو عرض شخص آخر، مثل إلقاء بنت على الأرض وفض بكارتها بالأصبع... إلخ.

هـ- الفعل الفاضح:

وهو فعل مادي يخدش في المرء حياء العين أو الأذن ويتضمن جرح الشعور العام لحياء شخص معين، واشتراط توافر العلانية مثل الأفعال والإشارات العلنية التي تقع من الجاني على نفسه (كممارسة العادة السرية أمام الجمهور) أو على جسم الغير فتخدش حياء المشاهدين.

و- انتهاك حرمة الآداب:

ويقصد بها صنع أو حيازة مطبوعات أو مخطوطات أو رسومات يدوية أو فوتوغرافية أو أمارات رمزية أو غير ذلك من الأشياء أو الصور العامة المنافية للآداب؛ وذلك بقصد الاتجار أو التوزيع أو اللصق.

ز- الإخلال بحياء أنثى:

ويرجع في تحديد الأفعال والألفاظ التي تقوم عليها الجريمة إلى العرف والبيئة، مع اشتراط وقوع الفعل في مكان عام أو مطروق.

٢- الجرائم الجنسية المثلية:

وهي سلوك جنسي يجرمه التشريع القائم في المجتمع ويعاقب عليه، ويكون السلوك الإجرامي موجهاً إلى الأشخاص الذين ينتمون إلى نفس الجنس، سواء كانوا رجالاً أم نساءً. وهذه الفئة من الجرائم نوعان: الأول: هو اللواط (Sodomy)، ويطلق على العلاقات الجنسية بين الذكور، والنوع الثاني: السحاق (Lesbianism)، ويطلق على العلاقات الجنسية بين الإناث.

ثالثاً: جرائم العنف:

وهي الجرائم التي يستخدم فيها كافة أشكال العدوان والعنف والإيذاء من أجل تحقيق أهدافها. ومن أهم هذه الجرائم:

١- جرائم القتل والإيذاء:

تشكل جرائم القتل والإيذاء النمط الشائع لغالبية الجرائم التي ترتكب ضد الأشخاص كما هو معروف في المصطلح القانوني. والواقع أن بواعث القتل أو الإيذاء كثيرة ومتعددة لا حصر لها فربما يقتل الفرد دفاعاً عن النفس أو دفاعاً عن المال أو دفاعاً عن الشرف، ربما يقتل بعمد مع سبق الإصرار، أو يقتل خطأ أو بإهمال، وربما يقتل استعمالاً لحق أو تنفيذاً لواجب.

٢- السرقة بالإكراه:

يقصد بها أخذ أي شيء ذي قيمة من السيارة أو في حيازة أحد أو مع شخص أو مجموعة من الأشخاص بالقوة، أو بالتهديد باستخدام القوة، أو العنف، أو وضع الضحية في موقف خوف، والسرقة بالإكراه إحدى جرائم العنف؛ لأنها تنطوي على استخدام القوة للحصول على النقود أو البضائع.

تعد السرقة بالإكراه إحدى جرائم الشارع (street crime)؛ لأنها نادراً ما تحدث في المنازل. فهي تحدث غالباً في الأماكن العامة مثل مواقف السيارات، والشوارع، والحدائق العامة.

٣- جرائم الكراهية:

ينظر الآن إلى جرائم الكراهية أو جرائم التحيز على أنها فئة جديدة من الجرائم الشخصية العنيفة. فهي عبارة عن أفعال عنفية توجه نحو شخص معين أو أعضاء جماعة ما؛ وذلك لأن هؤلاء الضحايا يشتركون في بعض الخصائص العنصرية أو العرقية أو الدينية أو خصائص النوع والتي تجعلهم موضع تمييز من قبل جماعة الأغلبية. ويمكن أن تشمل جرائم الكراهية انتهاك قدسية

دور العبادة أو المقابر، والمضايقات المتسمرة لأسر جماعات الأقلية السوداء التي بدأت تتحرك للسكن بجوار الأغلبية البيضاء في الولايات المتحدة الأمريكية، والدافع العنصري هو الذي يؤدي للإقدام على جريمة قتل لأحد الأفراد، والتي تصل أحياناً إلى قيام أحد الأفراد بقتل مجموعة من أعضاء جماعة عرقية أو عنصرية (١٨).

رابعاً: الجرائم الاقتصادية:

يرى الاقتصاديون أن الجريمة هي (التعدي على الموارد والثروات التي تقع في حيازة الأفراد والجماعات والدول). والجريمة التي ترتكب ضد الموارد الاقتصادية والثروات هي جريمة اقتصادية؛ لأن الجريمة هي سلوك معين له هدف عند المجرم الذي يرتكبها، فهو يستهدف تعظيم أرباحه عن طريق ما يحصل عليه من أموال الآخرين في حالة عدم القبض عليه. لهذا فالمجرم يعمل للتخطيط لجريمته حتى لا يقبض عليه أو حتى يمحي آثار الجريمة بقدر ما يستطيع(١٩).

تقسم الجرائم الاقتصادية إلى:

١- السطو إلى المنازل:

يعرف السطو على المنازل بأنه الهجوم على أحد المنازل التي يسكنها أناس آخرون ودخولها في وقت متأخر من الليل بنية ارتكاب جريمة بداخلها، ويعتبر السطو على المنازل جريمة خطيرة أكثر من كونها جريمة سرقة لأنه ينطوي غالباً على دخول منزل شخص آخر، وهو موقف يكون التهديد فيه بالضرر لقاطنيه وارداً وكبيراً. وحتى لو كان لا يوجد أحد أثناء السرقة، فإن احتمال الأذى للعائلة قائم عند إبلاغ الشرطة بالجريمة، لأن القانون يعتبر السطو على المنازل جناية. والسطو على المنازل يشبه السرقة بالإكراه في أنه هجوم أو اعتداء موجه ضد شخص معين (خصوصية المنزل) وضد الملكية.

٢- الجرائم المنظمة:

وهي أحد أنواع الجرائم الاقتصادية التي تقوم على تكوين مشروع إجرامي لجماعات من الأشخاص لتحقيق هدف طويل المدى هو الحصول على كسب اقتصادي من خلال الطرق والأساليب غير المشروع. ويقوم نظام المشروع الذي يتم تكوينه بإمداد المستهلكين بصورة مستمرة بالبضائع والسلع والخدمات المحرمة أو التي يجرمها القانون الجنائي، ويقيمون لها سوقاً متكاملاً وجاهزاً للدعارة أو البغاء، والأفلام والصور المنافية للآداب العامة، والقمار، والمخدرات.... إلخ.

هناك بعض السمات العامة للجريمة المنظمة والتي تميزها عن غيرها منها ما يلي:

١- الجرائم المنظمة عبارة عن نشاط تآمري، يتسم بالتآزر والتنسيق بين عدد كبير من الأشخاص في التخطيط للجرائم، وتنفيذ مختلف أشكال الأفعال غير المشروعة، أو متابعة وملاحظة الأهداف المشروعة من خلال الأساليب غير القانونية مثل التهديد من أجل الحصول على نصيب الأسد في بعض المشروعات التجارية.

٢- تهدف الجرائم المنظمة إلى تحقيق مكاسب اقتصادية في المقام الأول. هذا على الرغم من أن تحقيق المكانة والقوة ربما تمثل أيضاً عوامل دافعة.

٣- لا تقتصر أنشطة الجرائم المنظمة على تقديم الخدمات المحظورة قانوناً، ولكنها تشمل بعض الأنشطة الدقيقة والمهمة مثل الاستيلاء على أراضي الغير بالنصب والاحتيال، والزج بالنقود المزيفة في بعض الأعمال المشروعة.

٤- تستخدم في الجرائم المنظمة طرق وأساليب ضارية مثل التهديد والتخويف والعنف والرشوة والإفساد، وذلك من أجل إرضاء جشعها لبلوغ أهدافها والحفاظ على مكاسبها.

٥- تتسم الجماعات المتآمرة في الجرائم بالسرعة والفاعلية في التحكم في أعضائها وضبطهم تحت سيطرتها، وكذلك مع تابعيها وضحاياها.

٦- لا تشمل الجرائم المنظمة استخدام الإرهاب من أجل التغيير السياسي. فعلى الرغم من أن الأفعال العنيفة تمثل طرقاً رئيسة للجرائم المنظمة، نجد أن استخدام العنف لا يعني أن الجماعة الإجرامية جزء من تحالف المجرمين المنظمين (٢٠).

رابعاً: تقسيم الجرائم وفق عدد المحطات الرئيسة:

لقد قسّم المعنيون بشؤون الجريمة في المجتمع الجرائم في المجتمع وفق عدد من المحطات الرئيسة، يمكن الإشارة إلى أهمها بالشكل الآتي:

١- تقسيم الجرائم وفق جسامتها (نوعها):

هناك جنايات، وجنح، ومخالفات وذلك وفق العقوبة المقررة لكل نوع منها، وهذا التقسيم ليس ثابتاً ولكنه يختلف باختلاف الزمان والمكان، فما قد يعتبر جناية في وقت من الأوقات قد يصبح جنحة أو مخالفة في وقت آخر أو العكس؛ وذلك تبعاً للتغيير الذي يطرأ على القيم الاجتماعية السائدة أو طبيعة السلطة السياسية التي تملك التشريع، فإذا أصبحت الجماعة

المسيطرة لا ترى في فعل معين أنه ينافي نظمها أو يمثل خطورة عليها فإنها تجرم هذا الفعل، وكذلك إذا رأى المشرع أن العقاب على فعل يعده جريمة لا يتناسب مع خطورته أو ظروفه، فإنه قد يشدد العقاب عليه أو يخففه، وفي هذه الحالة يكون التخفيف مع إبقاء صفة الجريمة على حالها، أي أنها تظل جناية مثلاً، وقد تخفف العقوبة إلى الدرجة التي تغير من نوع الجريمة كنقلها من مرتبة الجنايات إلى مرتبة الجنح، وهذا ما يعرف بتجنيح الجنايات لظروف مخففة.

٢- تقسيم الجرائم وفق إيجابيتها وسلبيتها:

تقسم الجرائم إلى إيجابية وسلبية، فالفعل الإيجابي المخالف للقانون، كالقتل والسرقة والضرب والاغتصاب يعد جريمة إيجابية، أما الامتناع عن القيام بعمل يفرضه القانون، كالامتناع عن التبليغ عن بعض الجرائم، أو الامتناع عن دفع نفقة حكم على الشخص، فإنه يعد جريمة سلبية.

٣- تقسيم الجرائم وفق تعمدها:

الجريمة العمدية هي التي يتعمد فيها الجاني ارتكابها، وبعبارة أخرى هي الجريمة التي يتوافر فيها القصد الجنائي، أما الجرائم غير العمدية فهي التي لا يتوافر هذا القصد مثل القتل الخطأ، والإصابة الخطأ.

٤- تقسيم الجرائم وفق درجة استمرارها:

تقسم الجرائم إلى جرائم وقتية، وجرائم مستمرة، والجريمة الوقتية هي التي تتكون من فعل يحدث في وقت معين، وينتهي بمجرد ارتكابه كالقتل والتزوير، أما الجريمة المستمرة فهي تتكون من فعل متجدد ومستمر مثل جريمة خطف الأطفال أو سرقة تيار كهربائي.

٥- تقسيم الجرائم وفق موضوع ضررها:

تقسم الجرائم إلى جرائم ضارة بالمصلحة العامة كجرائم أمن الدولة، وجرائم ضارة بالأفراد كالقتل والسرقة (٢١).

٦- تقسيم الجرائم وفق أو حسب الآلات التكنولوجية الإلكترونية:

يمكن أن تقسم الجرائم الآن وفق الآلات والمعدات الإلكترونية الحديثة المستخدمة في تنفيذها مثل (الحاسب الآلي، الإنترنت... إلخ)، حيث اختلفت جريمة السرقة على سبيل المثال عن الماضي، إذ أصبحت السرقة الحديثة للأموال تتم عن طريق الإنترنت من خلال معرفة كلمة السر أو رقم

البطاقة الإئتمانية، أو جريمة توزيع المخدرات عبر الإنترنت أو جريمة القتل من خلال الإنترنت، وهذا النوع من الجرائم يطلق عليه في عصر المعلومات وتكنولوجياتها (بجرائم تكنولوجيا المعلومات).

٥- الأسباب والدوافع والعوامل وراء ظاهرة الجريمة.

بات مؤكداً أن أفراد الأسرة الواحدة يختلفون عن بعضهم البعض، وهذا الإختلاف أدى بالضرورة إلى اختلاف أفراد المجتمع الواحد، فهناك فروق فردية يتسم بها كل فرد عن الآخر، فعلى سبيل المثال: هناك العامل بجد وإخلاص، والعاجز والمتكاسل، والعاطل عن العمل وفي ذات الآن لديه القدرة على كسب المال وبطريقة مشروعة إذا توفرت الفرصة له.

بيد أن النفس الإنسانية أمّارة بالسوء إلا ما رحم ربي، وهذا الأمر جعل من أبناء المجتمع الإنساني، بل وعلى مستوى الأسرة الواحدة يعيشون حالة صراع مستمر من أجل الحصول على المال مرة، ومن أجل الانتقام وتعمد الأذى مرات عديدة.

تبقى الجريمة تشكل هاجساً مزعجاً لكل الناس، لاسيما أولئك المهتمين بشؤون الأمن وفرض القانون ومن هنا تم تقسيم الأسباب والدوافع وراء ظاهرة الجريمة وفق الآتي:

أولاً: العوامل البيئية:

يقصد بالعوامل البيئية مجموعة الظروف الخارجة ذات الصلة بالنواحي الاقتصادية والجغرافية والاجتماعية والحضارية التي تحيط بالإنسان وتؤثر في تكوين شخصيته وتحديد غاياته وأهدافه وتوجيه سلوكه وتصرفاته.

ليس كل الظروف التي تحيط بفرد ما داخله لزوماً في مضمونها. وإنما يدخل منها في هذا المفهوم الظروف ذات الصلة المباشرة أو غير المباشرة بشخص المجرم. أما ما عدا ذلك من الظروف فلا تندرج ضمن العوامل البيئية مهما كانت درجة قربها منه.

مميزات البيئة:

تتميز البيئة بخصيصتين هما:

أ- النسبية: ونسبية البيئة تعني أنها ليست واحدة بالنسبة لكل الأفراد. وإنما تختلف من فرد لآخر حسب درجة اتصاله بالظروف الخارجية وتأثره بها.

بناءً على ذلك، فإن العناصر البيئية لفرد ما لا تدخل كلها أو بعضها ضمن العناصر البيئية لغيره. فهي - أي البيئة - تختلف من شخص لآخر، حتى بالنسبة للأشقاء الذين يعيشون في كنف أسرة واحدة. وهي أيضاً تختلف بالنسبة للشخص الواحد باختلاف الزمان والمكان. فبعض الظروف تؤثر على شخص معين في حقبة من حياته، ويفقد تأثيره في حقبة أخرى منها. ومن ثم يعد عاملاً بيئياً بالنسبة للأولى ولا يعد كذلك بالنسبة للثانية.

ب- التكامل:

يعني تكامل البيئة أنها واحدة لا تقبل التجزئة. فالعوامل البيئية لا يحدث أثرها فرادى على الشخص وبالتالي على سلوكه، وإنما تتضافر فيما بينها لتباشر تأثيرها. ومؤدّى ذلك أن تخلف أحد هذه العوامل يفضي إلى احتمال اختلاف تأثيرها عليه. وبناءً على ذلك لا يمكن القول: إن سلوكاً معيناً، هو ثمرة لعامل بيئي واحد. كما لا يمكن الجزم بأن عاملاً بيئياً معيناً يؤثر على نحو معين على الشخص، إذ قد يضمحل أثر هذا العامل أو يتلاشى تماماً بسبب وجود عامل آخر، كما قد يعزز هذا العامل بقية العوامل ويشد من أزرها في مباشرة تأثيرها عليه. لكن الذي لا ينبغي أن يغيب عن البال أنه إذا كان من اللازم تضافر العوامل البيئية على صعيد واحد كي تنتج أثرها في توجيه السلوك الإجرامي، فإنه من اللازم أيضاً انضمام العوامل الفردية إليها؛ ذلك لأن العوامل البيئية لا تقوى على التأثير على الشخص وتوجيه سلوكه وجهة إجرامية بمعزل عن العوامل الفردية.

أنواع العوامل البيئية:

يمكن تقسيم العوامل البيئية بحسب الوجهة التي ينظر منها إليها، إلى الأقسام الآتية:

أ- من حيث طبيعتها: تقسم إلى:

١- عوامل مادية: كمجموعة الزملاء في المدرسة أو النادي أو العمل.

٢- عوامل معنوية: مثل العادات والتقاليد والتعليم.

ب- من حيث نطاقها: تقسم إلى:

١- ظروف عامة تباشر تأثيرها على كل أفراد المجتمع أو معظمهم، ومثالها: العوامل الطبيعية والاقتصادية والسياسية.

٢- ظروف خاصة تباشر تأثيرها على شخص واحد أو على مجموعة قليلة من الأشخاص. كظروف الفرد المالية كالفقر والغنى وظروفه التعليمية، كالجهل أو التعليم.

ج- من حيث دوامها: فهي تقسم إلى:

١- عوامل متسمرة: أي عوامل تدوم وقتاً طويلاً نسبياً، كالنظام السياسي والاقتصادي والقيم التي تسود المجتمع.

٢- عوامل مؤقتة: وهي عوامل وقتية كنجاح الإنسان في اختبار ما أو رسوبه فيه. أو وفاة أحد أفراد عائلته. وهذا الصنف من العوامل يختلف بأختلاف الظروف الفردية، إلا أن تأثيره على السلوك الإجرامي لا يمكن تجاهله البتة.

د- من حيث الموقف الإداري الفردي تجاهها: تقسم إلى العوامل البيئية إلى:

١- عوامل مفروضة: ومثالها الأسرة التي ينشأ في كنفها الشخص.

٢- عوامل عابرة: ومثالها مجتمع المدرسة.

٣- عوامل مختارة: ومثالها الزواج أو الفراق (٢٢).

*** العلاقة بين العوامل الطبيعية والسلوك الإنساني:**

يقصد بالعوامل الطبيعية: هي مجموعة الظروف الجغرافية التي تسود في منطقة معينة مثل حالة الطقس من حرارة وبرودة، وكمية الأمطار، ونوع ودرجة الرياح وطبيعة الأرض والتربة.

أما عن العلاقة بين الطبيعة والسلوك، فلقد تنبه الفلاسفة منذ قديم الزمان إلى تأثير الوسط الطبيعي لمنطقة معينة على سلوك من يعيش عليها من الناس. ونادوا بضرورة التوافق بين القوانين السارية فيها وظروفها الطبيعية.

وإظهاراً للعلاقة بين الطبيعة الجغرافية والأنماط السلوكية للبشر قال هردر (HERDRE): إن تاريخ شعب من الشعوب لا يعدو أن يكون الطبيعة الجغرافية لهذا الشعب في حركتها عبر العصور. ويمتد تأثير الوسط الطبيعي إلى تكوين المجتمع ذاته؛ فيؤثر في حضارته، وثقافته، واقتصاده، بل والعادات والتقاليد التي تسود فيه. وهي عوامل ينعكس تأثيرها بالضرورة على الظاهرة الإجرامية.

*** أثر الأحوال المناخية على الظاهرة الإجرامية:**

يقصد بالأحوال المناخية: حالة الطقس من حرارة وبرودة وأمطار ورياح. وقد دلّت الدراسات الإحصائية على وجـود صلة بين الأحوال المناخية والجريمة، وبيان ذلك:

١- ففي دراسة أجريت على أثر حرارة الجو على الجريمة شملت شمال إيطاليا وجنوبها أظهرت اختلاف ظـاهرة الإجـرام في الشمال، حيث برودة الطقس، عنه في الجنوب؛ إذ يكون الطقس حاراً.

٢- وفي دراسة مماثلة على الإجرام في شمال فرنسا مقارنة بالجنوب خلال الفترة من عام (١٨٢٥-١٨٣٠) خلص جيري إلى أن كل مائة جريمة من جرائم العدوان على الأشخاص يقابلها مائة وواحد وثمانون جريمة من جرائم الاعتداء على الأموال في الشمال الفرنسي، في حين أن كل مائة جريمة من جرائم الاعتداء على الأشخاص يقابلها (٤٨.٨) جريمة من جرائم الاعتداء على الأموال في جنوبه. وانتهى إلى وضع الصياغة الأولى لما أطلق عليه (قانون الحرارة الإجرامي)، والذي يقول فيه: إن جرائم الاعتداء على الأشخاص تزداد نسبتها في المناطق الجنوبية أثناء الفصول الحارة، وأن جرائم الاعتداء على الأموال تغلب نسبتها في المناطق الشمالية وأثناء فصول السنة الباردة.

٣- وانتهى الفقيه (لاكساني) في تقويمه الخاص عن الجريمة في فرنسا خلال الفترة من (١٨٢٧-١٨٧٠) موزعة على فصول السنة إلى القول: بأن هناك علاقة مباشرة بين الجرائم ضد الأشخاص من ناحية ودرجات الحرارة المرتفعة وطول نهار اليوم من ناحية أخرى. كما توجد علاقة مباشرة أيضاً بين الاعتداء على الملكية من ناحية وانخفاض درجة الحرارة وطول ساعات الليل من ناحية أخرى.

*** تفسير العلاقة بين المناخ والجريمة:**

تفرّق رأي العلماء - تفسيراً للعلاقة بين المناخ والجريمة - إلى ثلاثة اتجاهات رئيسة وذلك على النحو الآتي:

أ- النظرية الطبيعية:

ذهب أنصار هذه النظرية إلى الإقرار بوجود صلة مباشرة بين المناخ والجريمة قولاً بأن اختلاف حالة المنـاخ؛ يـستتبع اختلاف نوع السلوك الذي ينتهجه الأفراد بما في ذلك السلوك الإجرامي، لكنهم ذهبوا في بيان ذلك مذاهب شتّى منها:

١- فمنهم من اتجه إلى القول: بأن ارتفاع درجة الحرارة يزيد من حيوية الإنسان ونشاطه على نحو يجعله أكثر استعداداً للإثارة والاندفاع.

مع توقد في العاطفة، وفرط تيقظ في الغريزة الجنسية، وميل جارف إلى الجنس الآخر. وهذا من شأنه أن يقدم العديدون على جرائم العدوان على الأشخاص والأعراض.

تفسيراً لذلك يقول العلامة فيري (Ferri): إنه نتيجة لارتفاع درجة الحرارة فإن الطاقة الحرارية التي يولدها الجسم، بسبب ما يتناوله الإنسان من غذاء تفيض عن حاجته، فيترتب عليها زيادة في اندفاعه وحدته.

بينما فسّر العالم الألماني فولدس (Foldes)، ذلك بالقول: إن زيادة الحرارة توهن قدرة الإنسان على مقاومة الدوافع اللاّأخلاقية، فينجرف نحو ارتكاب الجرائم وبصفة خاصة تلك الماسة بالعرض والأخلاق.

٢- ومنهم من اتجه إلى تفسير تأثير الضوء على الظاهرة الإجرامية بالقول: بأنه في فصل الشتاء يطول الليل ومن ثم الظلام، وهذا الأخير يُيسّر الإقدام على الإجرام ويوضح علة زيادة السرقات في الفصل المذكور، مقارنة بغيره من الفصول.

ب- النظرية الاجتماعية:

يُسلّم أنصار هذه النظرية بوجود صلة غير مباشرة بين التغيرات المناخية والظاهرة الإجرامية، على سند من القول: بأن المناخ يحدث أثره الدافع إلى الجريمة، من خلال الحياة الاجتماعية للناس، وتفصيل ذلك:

١- إن زيادة جرائم الاعتداء على الأشخاص صيفاً مقارنة بالشتاء يرجع إلى أمرين هما:

الأمر الأول:

يكمن في احتكاك الناس بعضهم ببعض نتيجة تركهم منازلهم وتجمعهم في الحدائق والطرقات والأماكن العامة تمضية لأوقات فراغهم.

الأمر الثاني:

تعطل طاقة الإنسان عن العمل إبان إجازته الصيفية وتغير وجهتها صوب الاعتداء على الغير، ويحصل ذلك بكثرة في الأماكن المزدحمة، وفي الأسواق. وعلى صعيد آخر: فإن حرارة الجو تدفع

الناس إلى تناول المشروبات ومنها الخمور، وقد يسرف البعض ولا يجدوا متنفساً لسكرهم إلا بالعدوان على غيرهم.

٢- أما زيادة جرائم الأموال في الشتاء عنها في الصيف فمرده - لدى أنصار النظرية الاجتماعية - ازدياد متطلبات الناس في الشتاء مقارنة بمتطلباتهم في الصيف، فهم يحتاجون الغذاء والكساء بكثرة لمواجهة برودة الجو، كما يحتاجون إلى المسكن ووسائل التدفئة اللازمة، وهي أمور تحتاج إلى وفرة مالية قد لا تكون متحققة لدى بعضهم مما يدفع بهم نحو ارتكاب جرائم الأموال؛ عساهم يحصلون على ما يسد حاجاتهم، ويفي متطلباتهم.

هذا بالإضافة إلى ما تعانيه بعض المناطق من ركود اقتصادي في فصل الشتاء على نحو يفضي إلى ارتفاع نسبة البطالة فيها، وهذه الأخيرة - مقرونة بالحاجة- تعتبر عاملاً دافعاً لارتكاب الجرائم الماسة بالأموال.

ج- النظرية العضوية النفسية:

يؤكد دعاة هذه النظرية على أن العلاقة بين تعاقب فصول السنة وبين الإجرام علاقة مباشرة. وهي تحصل نتيجة للتغيرات الدورية في أداء أعضاء الجسم لوظائفها بتأثير التقلبات الجوية، وما يستتبع ذلك من تغير في الاتجاهات النفسية. ويلحظ أثر هذه التغيرات بوضوح في الجرائم الجنسية التي تبلغ أقصى معدلاتها في فصل الربيع.

لقد رأى أنصار هذه النظرية أن وظائف الجسم تصل إلى أقصى حدّتها في فصل الربيع، ولا غرابة في هذا الأمر؛ فالحيوان والنبات، كذلك يعتبر الربيع موسماً لتزاوجها، والإنسان مثلها يخضع لتأثير العوامل المناخية ويرتكز هذا التأثير - خلال فصل الربيع - في أجهزته ومشاعره ومن ثم غريزته الجنسية وهو ما يؤدي إلى كثرة الجرائم المرتبطة بها ممثلة في الجرائم
الخلُقية (٢٣).

ثانياً: الأسباب الاجتماعية:

١- ضعف الوازع الديني:

لقد كانت العقيدة الإسلامية في عصر الإسلام الأول موقظة الضمير مهذبة النفس؛ لأنها كانت بالدرجة الأولى شعوراً قوياً بموقع الإنسان من خالقه وإلهه الواحد الأحد الذي لا إله سواه، وهو موقع المسؤول عن أمانة إستخلافية في هذه الأرض، ولقد كانت العقيدة الإسلامية متصلة

بحياة الفرد المسلم النفسية والخلقية، والحياة الاجتماعية والاقتصادية والثقافية والعلمية. فكانت الجريمة نادرة الوقوع، وإن وقعت، فإن آثارها سرعان ما تتلاشى وتنتهي في مهدها نظراً لقوة تمسك المجتمع بعقيدته الإسلامية.

ما أن ضعف الالتزام بالعقيدة الصحيحة وبرز الانحراف وظهرت المؤثرات السلبية في المجتمع الإسلامي حتى أصبح التسابق نحو الشهوات الذاتية، والرفاهية الشخصية، أمراً واضحاً. حتى أصبح العديد من أفراد المجتمع لا يهمهم إلا الحصول على المال بأي طريق مشروع أو غير مشروع، حلال أم حرام.

كما كثر التنازع على الأموال والحقد والحسد بين أفراد المجتمع والتسابق على مظاهر الحياة الخادعة، والانصراف عن جوهر الدين الإسلامي، والعادات والقيم الإسلامية والعربية الأصيلة. كل ذلك يجعل أفراد المجتمع يعيشون فراغاً روحياً وعاطفياً، وبالتالي الانحراف والفساد والتصرف دون وازع من دين أو ضمير أو خلق فيرتكب الجرائم من قتل أو فواحش محرمة أو تدمير أو تخريب أو غير ذلك. ولا علاج لذلك إلا بالعودة إلى تحكيم شرع الله والتمسك بالعقيدة الصحيحة.

ضعف المستوى أو الدور التربوي للأسرة:

الأسرة هي الخلية الأساسية لبناء المجتمع، وإذا صلحت صلح المجتمع وبفسادها يفسد المجتمع؛ وقد أعطى الإسلام دوراً كبيراً ومهماً للأسرة منذ اللحظة الأولى في تكوين الأسرة باختيار الزوج الصالح والزوجة الصالحة، يقول الله تعالى: (ولأمة مؤمنة خير من مشركة ولو أعجبتكم) فهذه المفاضلة في اختيار الزوجة مبنية على سلامة العقيدة والخلق والاتجاه قبل الوضاءة والجمال، وهذا لا يعني إهدار قيمة الجمال في الزوجية، بل قال الرسول صلى الله عليه وسلم: (تنكح المرأة لأربع: لمالها ولحسبها ولجمالها ولدينها فاظفر بذات الدين تربت يداك) فاعتبار الدين يعني رغبة الإسلام في استقرار الأسرة، وصلاح المرأة فيه سعادة الأسرة والمجتمع (فالدين هو مطمح نظر الإنسان المسلم في كل شيء لا سيما فيما تطول صحبته كالزوجة).

هكذا يوصي الإسلام في اختيار الزوجة الصالحة الودود الولود، كما يوصي باختيار الزوج الذي يجمع بين صفات الإنسانية الفاضلة وأخلاق الرجولة المكتملة والذي ينظر إلى الحياة نظرة صادقة مستقيمة من خلال الإيمان بربه، فالأسرة هي التي تقع عليها المسؤولية الأولى في تربية

الأجيال وبناء المجتمعات، فإذا قامت بدورها تجاه أبنائها فإنها تساهم بشكل مباشر في خلق مجتمع صالح. وإذا تقاعست أو عجزت عن دورها التربوي ضاع أفرادها وضاع معهم المجتمع.

يحدث غالباً هذا العجز والتكاسل عن الدور التربوي للأسرة من انشغال رب الأسرة بأعماله الخاصة والركض وراء المادة طيلة الوقت بما لا يترك وقتاً معيناً لقضائه مع أفراد أسرته وتوجيههم إلى ما ينفعهم في دنياهم وآخرتهم، فيعجز عن دوره الأساسي كمربي وموجه وقائد أسرة. كما أن خروج المرأة من بيتها وإعطائها جل وقتها للعمل خارج المنزل أو التسوق أو لقضاء أوقات طويلة خارج البيت وترك مسؤولية البيت وتربية الأبناء والبنات للخدم ذوي الثقافات المختلفة التي تتباين مع أساليب ومبادئ التربية الإسلامية مما جعل دور الأسرة ضعيفاً وهامشياً.

كما أن اختلاف طرق وأساليب التربية للأبناء من جيل إلى جيل يؤدي إلى عدم التوافق والانسجام مما يهيء الفرصة لسلوك طرق غير مناسبة لا تتماشى مع النمط الاجتماعي مما يسهل الفرص الكبيرة لارتكاب الجرائم.

٣- تدني الدور التربوي للمدرسة:

المدرسة هي المؤسسة التربوية الثانية بعد البيت في بناء المجتمع، حيث بدأت تقوم بدروها وهي في المسجد، ثم أصبح لها استقلالية ونظاماً استخدمت فيه كافة وسائل التربية والتعليم والثقافة والأخلاق. إلا أن دورها في عصرنا الحاضر انحصر في العملية التعليمية غالباً، وأصبح تركيز أعضاء المدرسة من المديرين والمعلمين فيها والموجهين والمرشدين على الجانب التعليمي دون ربطه بالواقع العملي التطبيقي في حياة الأمة الإسلامية المعاصرة، رغم ما تحتويه المناهج من ثقافة واسعة ومصارف جمة إلا أن التطبيق لتلك المبادئ ليس له قدوة في المدرسة أو خارجها وليس له متابعة من الأسرة في المجتمع، فضعف تقدير المنهج والمعلم. وزاد من الضعف لدور المدرسة في عصرنا الحاضر، كثرت السلوكيات التي يتم اكتسابها من وسائل الإعلام المختلفة التي تبث برامج للثقافات المختلفة عن بيئتنا، إضافة للتأثيرات المباشرة للعمالة والجاليات الوافدة من خارج الوطن مما أثر على أفراد المجتمع وزاد في نمو الجريمة وكثرة ظواهر الانحراف في المجتمع.

٤- عدم ترشيد وسائل الإعلام:

تقوم وسائل الإعلام بدور كبير في توجيه أفراد المجتمع ويسري تأثيرها بشكل واضح على قطاع كبير من أفراد المجتمع، لا سيما بعد ظهور الأجهزة الفضائية والبث المستمر للمواد الإعلامية غير المرشدة وغير النافعة والتي لا تتفق مع مبادئ وقيم المجتمعات الإسلامية، إضافة إلى

ما تنشره المجلات الخليعة من صور الإباحية وتحريض على العلاقات الجنسية المحرمة وطرق الرذائل والانحراف والتي يتم تغليفها في صورة العلاقات الإنسانية والحرية الشخصية، وكان الأجدر بوسائل الأعلام في البلدان الإسلامية أن لا تسير على تلك المناهج التي سلكتها وسائل الإعلام الغربي أو الشرقي المدمر، وأن تقوم ببث البرامج الهادفة والتي تتميز بالأخلاقيات الإسلامية الفاضلة، والعلاقات الاجتماعية المباحة، وأن تعمل ليل نهار على نشر مبادئ وقواعد الدين الإسلامي والثقافة الإسلامية لكافة مستويات المجتمع صغاراً وكباراً، وأن تخرج من الاستديوهات المغلقة إلى ميادين العمل المختلفة وعرض مشكلات المجتمع المعقدة والبحث عن حلول مناسبة لهذه المشكلات سواء كانت اجتماعية، أو ثقافية أو اقتصادية، إضافة إلى طرق برامج التدريب والتعليم المختلفة بالقنوات والبرامج الإرشادية في مختلف القطاعات الاقتصادية والاجتماعية.

٥- المخدرات وشرب المسكرات:

إن تعاطي المخدرات وشرب المسكرات والتي هي أم الخبائث سبب رئيسي في ارتكاب الجرائم بمختلف أنواعها، بل إن أضرارها على الدين والخلق والصحة والمجتمع والاقتصاد بالغة الأثر، وهي نتيجة طبيعية لارتكاب أو تعاطي ما حرّم الله. فالله إنما حرمها لضررها.

تغتال المخدرات والمسكرات العقول، وتفتك بها وتؤثر على الفرد، وتدمرها ويؤدي بعضها إلى افتقاد المروءة والخلق، وتؤدي إلى الفوضى واختلال نظام المجتمع، ويقل إنتاج الفرد المتعاطي لها، فتقل قدراته العقلية والإنتاجية، ولا يعود صالحاً للعمل؛ لأنه أصبح شخصاً غير سوي وغير موثوق به فيرتكب من الجرائم والحوادث والانحرافات العديدة، وينصرف عن العمل والإنتاج فيقل دخله المالي أو يصبح بلا دخل. وبالتالي يزيد توتره فيصبح عالة على المجتمع، يزيد في نسبة البطالة ويفقد أعصابه وتكثر مشكلاته مع أهل بيته وأولاده وجيرانه، فيعتدي بالضرب والسرقة ولو استطاع بيع أحد أبنائه أو زوجته لفعل مقابل الحصول على المخدر.

كما تدفع المخدرات بالمدمنين عليها الذين لا يستطيعون الإنفاق من أجل الحصول عليها إلى الاعتداء على أموال الغير، والتخريب والإرهاب والتدمير مقابل أجر معين من قبل أصحاب الاتجاهات الفاسدة والعناصر الهدامة المزعزعة لأمن المجتمع.

٦- عدم الاستقرار الاجتماعي:

إن عدم الاستقرار الاجتماعي وعدم وجود تنظيم اجتماعي منضبط أو عدم تطبيق النظام الاجتماعي الإسلامي العادل، كذلك تنوع الاتجاهات والقيم والعادات، وقلة التماسك والترابط

الأسري للأفراد أدّى إلى حالات من الفوضى والتناقض في التنظيم الاجتماعي والقيم والأهداف، كما أن الاختلال في التوازن بين الجانبين المادي والمعنوي في كثير من المجتمعات بدرجة كبيرة يساهم في زيادة معدل الجريمة حيث التفاوت الطبقي في المجتمع مما أدّى إلى ثراء بعض المقربين من الحكومات على حساب أبناء المجتمع، ممّا هيّأ المناخ الملائم إلى ظهور الجريمة الاقتصادية والحقد على تلك الفئات المقربة في العديد من بلدان العالم الإسلامي (٢٤).

ثالثاً: الأسباب الاقتصادية:

هنا لا يمكن حصر كافة الأسباب الاقتصادية الدافعة للجرائم ولكن يمكن أن نقدم أهم الأسباب التي تدفع سواء بشكل مباشر أو غير مباشر إلى ارتكاب الجريمة، ومن تلك الأسباب ما يلي:

١- الفقر:

إن الفقر داء خبيث إذا تغلغل في مجتمع أدى إلى هلاكه وتدميره، وازدادات معه العقبات الاقتصادية المترابطة، والفقر عقبة كبرى في وجه التنمية في العالم، حيث تعاني (٥٤) دولة نامية من دول العالم الثالث من انخفاض الدخل المتوسط خلال عقد الثمانينات منها (١٤) دولة تعيش على حافة الفقر. إضافة إلى تصاعد المديونية لهذه الدول. وفي كل عام يموت أكثر من (١٤) ميلون طفل قبل سن الخامسة بسبب الفقر ويعاني حوالي (١٥٠) مليون طفل من سوء التغذية.

يعد الفقر سبب مباشر من أسباب الجرائم؛ لأن عدم توفر الأمن الاقتصادي، وسوء الغذاء والكساء والرعاية الاجتماعية الضرورية أدّى إلى تكوين اتجاهات خطيرة تنحو إلى معارضة المجتمع والتمرد عليه. وقد انتهت دراسات في علم الاجتمع الجنائي إلى وجود علاقة قوية بين الفقر والجريمة، حيث كان الفقر سبب رئيسي في الإجرام، فقد كان (٢٧%) من المنحرفين ومرتكبي الجرائم يرجع إلى الأسر الفقيرة، وتشير نتائج العديد من البحوث إلى زيادة معدلات الجريمة بين المجرمين الذين ينتمون إلى الطبقات الفقيرة. حيث تشير كذلك إلى بطالة المنحرف قبل ارتكابه للجريمة وعدم كفاية دخله أو دخل أسرته. وفي الشريعة الإسلامية استعاذ الرسول (صلى اللـه عليه وسلم) من الفقر. وورد عن علي - كرّم اللـه وجهه - قوله: (لو كان الفقر رجلاً لقتلته).

٢- البطالة:

تؤكد الدراسات الميدانية بوجود علاقة قوية بين البطالة والجريمة في العالم العربي، كما أن النظام الاقتصادي الرأسمالي المطبق في المجتمعات الرأسمالية رغم الرخاء الذي يعيشه لم يتمكن

من القضاء على البطالة التي تعتبر من أهم العوامل الاقتصادية التـي تـؤدي إلى ارتكـاب الجريمـة لاسـيما الجـرائم الاقتصادية.

٣- الهجرة:

يترتب على النمو الاقتصادي هجرة أفراد المجتمع من المناطق الريفية - الفقيرة - إلى المنـاطق الـصناعية، بحثـاً عـن فرص عمل أفضل حيث تزداد هذه الفرص مع التقدم الاقتصادي في مناطق الجذب السكاني.

بينما تنعدم فرص العمل وينتشر الكساد في مناطق الطرد الـسكاني، فالعلاقـة طرديـة بـين حجـم الجريمـة وأنماطهـا ومنطقة الجذب السكاني، وعلاقة عكسية بين حجم الجريمة ومنطقة الطرد السكاني.

كلما زادت عوامل جذب السكان في المنطقة كلما زاد حجم الجريمة وأنماطها، فالعلاقـة هنـا علاقـة طرديـة؛ وكـذلك كلما نقصت العوامل التي تجذب السكان للمنطقة ينخفض معدل الجريمة. وبالمقارنـة نجـد أن منطقـة الطـرد الـسكاني تنخفض فيها الجريمة، حيث أن العلاقة بين حجم الجريمة وعوامل منطقة الطرد السكاني علاقة عكسية.

كما أن الهجرة عامل من عوامل عدم الاستقرار الاجتماعي للعاملين والذي يؤثر على نفـسية كـل مغـترب في المهجـر وأسرته في الوطن، إضافة لاختلال التركيب الاجتماعي، حيث تزداد نسبة النساء والأطفال بين المقيمين وفي ظل غيـاب رب الأسرة يحرم الأبناء من الإشراف والتوجيه، وتحمل العبء الزوجة، ويـؤدي ذلـك إلى انحـراف الأبنـاء لعـدم قـدرتها عـلى التوجيه والإرشاد والمتابعة المستمرة، وربما يمتد الانحراف إلى بقية أفراد الأسرة.

٤- ارتفاع تكاليف المعيشة:

يعد ارتفاع تكاليف المعيشة في العديد من بلدان العالم، ودون أن يتحقق الارتفاع المناسب في دخـول الأفـراد يـؤدي إلى ارتكاب الجرائم. كمحاولة التهرب من سداد الضرائب، أو الرسوم الجمركية بالاتفاق مع بعض الموظفين المسؤولين عن هذه الأعمال مقابل رشوة، وهذا نتيجة للانحراف بالوظيفـة العامـة مـن أجـل الحـصول عـلى زيـادة في الـدخل وكـذلك استغلال الوظيفة العامة في الحصول على ربح أو منفعة، وانتشار الفوضى في الإدارة والمجتمع.

٥- الاحتكار والاستئثار والأنانية:

إن الأنظمة الاقتصادية الوضعية المطبقة في المجتمعات الغربية والشرقية، مسؤولة بشكل كبير جداً عن حدوث الجرائم فالأنانية والاستئثار وحب السيطرة الفردية في النظام الرأسمالي وكذلك الاستئثار بالسوق والتحكم في الإنتاج وفرض سلع وخدمات رديئة على المستهلكين، والبيع والشراء بأسعار سياسية لا علاقة لها بالأسعار الاقتصادية في النظام الاشتراكي، وكل ذلك أدى إلى زيادة معدل الجريمة، بظهور العديد من الظواهر الاقتصادية المؤدية إلى ارتكاب الجرائم، مثل تدهور الإنتاجية وانخفاض معدل النمو للدخل القومي، ومن ثم ارتفاع معدلات البطالة، واشتعال معدلات التضخم.

٦- زيادة الدخل:

أدت التنمية الاقتصادية في العديد من بلدان العالم إلى زيادة الدخول الفردية، وزيادة عدد المشروعات والشركات وزيادة الإنتاج، وزيادة التحضر فرادت جرائم السرقة والنصب والاحتكار والاحتيال والرشوة التزييف واتلاف الموارد، (ومن الأمثلة على ذلك ما حصل في دول الخليج العربي من طفرة اقتصادية، بعد عملية التنمية الاقتصادية التي زادت معها المشروعات والشركات) ولاستقطاب أيدي عاملة كبيرة من مختلف الجنسيات إضافة إلى استقطاب أيدي عاملة للخدمات العامة والخاصة على حد سواء، نتيجة لزيادة الدخل.

إضافة إلى العديد من حالات السرقة والنصب والاحتيال التي حصلت في هذه البلدان من بعض العمالة المنزلية الوافدة والتي وصلت إلى حد القتل والاعتداء على أصحاب الأموال والأعمال.

كما أن معظم المدن الكبيرة في الدول الغنية تضم أعداداً متزادية من المواطنين المعدمين الذين يشكلون طبقة دنيا تهدد بالخطر، فمعظمهم بلا عمل ولا مال فهم يحسدون الأغنياء ويحقدون عليهم، وهم على استعداد في معظم الأحوال للاتجاه إلى الجريمة لتحسين دخلهم الذي لا يزيد عن حد الكفاف، ومن المنتظر أن تشهد العديد من مدن العالم في الأمم الغنية والفقيرة براكين اجتماعية قد تنفجر ما دامت الفجوة قد ظلت واسعة بين الغالبية من الجماهير المعدومة. ولهذا كانت الدخول المرتفعة والسعي لزيادة الدخل المنخفضة لدى بعض الفئات سبب رئيسي لارتكاب الجرائم الاقتصادية.

٧- السياسيات النقدية والمالية غير العادلة:

إن إتباع سياسات نقدية أو مالية غير عادلة أو غير متزنة يؤدي إلى ارتكاب الجرائم الاقتصادية؛ وذلك مثل سياسة التوسع في الإصدار النقدي والإفراط فيه يؤدي إلى التضخم، وارتفاع الأسعار وانخفاض الدخول الحقيقية وعدم كفايتها لتحقيق المطالب الأساسية، وتدهور القوة الشرائية للنقود وانعدام دورها في تسوية المدفوعات الآجلة وتأثير ذلك على المعاملات والديون، وعلى أصحاب الدخول الثابتة ويصاحب التوسع في الائتمان المصرفي مع عدم الرقابة الجيدة لتزايد حالات السرقة والاختلاس في قطاع المصارف والمماطلة في سداد القروض.

كما أن التقديرات الجزافية المبالغ فيها للضرائب أو رسوم الخدمات من جانب الأجهزة الحكومية المختصة تؤدي إلى هروب رجال الأعمال عن دفعها. وشعور لدى المواطنين بثقل هذه الأعباء المتزايدة عليهم، فصاروا يعمدون للتحايل على الدولة وموظفيها بعدم دفعها.

يعتبر غياب الرقابة الجادة على السياسات والبرامج التنموية والمشروعات والتي يصاحبها تنفيذ بعض المشروعات التي لا تمثل ضرورة للمجتمع ولا تحقق عائداً اجتماعياً؛ نتيجة لفساد بعض القائمين على إدارة القطاع، وحيث يتم إقامة مشاريع غير مدروسة والحصول على عمولات مالية كبيرة مقابل رشوة، أو تأمين معدات لا تصلح للغاية المشتراة لها، وهذا فيه فساد كبير وقد يؤدي ذلك إلى زيادة العجز في موازين المدفوعات والذي يعتبر سبباً في زيادة الجريمة في الدول النامية والتي تتبع سياسات اقتصادية ونقدية ومالية غير عادلة (٢٥).

بناءً على كل ما تقدم، تبقى العوامل الاقتصادية تشكل هاجساً مخيفاً، بل ومقلقاً لكل من رجال الأمن والقانون والمجرم، فكلاهما يريد أن يقوم بعمل ما، إلاّ أن القاسم المشترك بين الاثنين هو الإنسان، فمن يغلب مَن؟!

هوامش الفصل الأول:

١- سليمان عبد المنعم: أصول علم الإجرام والجزاء. ط٢. بيروت المؤسسة الجامعية، ١٩٩٩ ص (١٢٣-١٢٤).

٢- سعد المغربي، السيّد أحمد الليثي. المجرومون. القاهرة، المركز الإسلامي للطباعة والنشر، ١٩٦٧. ص (١٠٣-١٠٥).

٣- المرجع السابق نفسه. ص (١٠٦).

٤- علي محمد جعفر: الأحداث المنحرفون، دراسة مقارنة. ط٣. بيروت: المؤسسة الجامعية للدراسات والنشر والتوزيع، ١٩٩٦. ص (٥).

٥- سعد المغربي، السيّد أحمد الليثي: مرجع سابق، ص (١٠٧-١٠٩).

٦- المرجع السابق نفسه. ص (١٠٩-١١٠).

٧- رؤوف عبيد: أصول علم الإجرام والعقاب. ط ٨. القاهرة: دار الجيل، ١٩٨٩. ص (٢٧٠-٢٧١).

٨- ابن منظور: لسان العرب، مادة جرم.

٩- سورة هود: الآية [٨٩].

١٠- سورة المائدة: الآية [٨].

١١- خلف بن سليمان بن صالح النمري: الجرائم الاقتصادية وأثرها على التنمية في الاقتصاد الإسلامي. الإسكندرية: مؤسسة شباب الجامعة، ١٩٩٩. ص (٥).

١٢- سليمان عبد المنعم: مرجع سابق. ص (٦١-٦٢).

١٣- عبد الرحمن محمد أبو توتة: بيروت: الجامعة المفتوحة، ١٩٩٤. ص (٢٦-٣٠).

١٤- محمد شحاتة ربيع، جمعة سيد يوسف، معتز سيد عبد الله: علم النفس الجنائي. القاهرة: دار غريب، ١٩٩٤ ص (٣٩-٤١).

١٥- المرجع السابق نفسه. ص (١٥١-١٦٦).

١٦- سليمان عبد المنعم: مرجع سابق. ص (٣٥٠-٣٥٣).

١٧- المرجع السابق نفسه. ص (٣٥٤-٣٥٧).

١٨- محمد شحاتة ربيع، جمعة سيّد يوسف، معتز سيد عبد اللـه: مرجع سابق. ص (١٧٥-١٩٢).

١٩- خلف بن سليمان بن صالح النمري: مرجع سابق. ص (٦).

٢٠- محمد شحاتة، جمعة سيد يوسف، معتز سيد عبد اللـه: مرجع سابق. ص (١٩٢-١٩٥).

٢١- محمد شفيق: الجريمة والمجتمع: محاضرات في الاجتماع الجنائي والدفاع الاجتماعي: الإسكندرية: المكتب الجامعي الحديث (د.ت) ص (١٨-٢٠).

٢٢- حاتم بكارّ: الاتجاهات المعاصرة في استقصاء عوامل الإجرام وتقويم المجرمين. الإسكندرية: منشأة المعارف، ٢٠٠١. ص (١٠٥-١٠٧).

٢٣- المرجع السابق نفسه، ص (١٠٧-١١٣).

٢٤- خلف بن سليمان بن صالح النمري: مرجع سابق. ص (٩-١٣).

٢٥- المرجع السابق نفسه. ص (١٣-١٩).

الفصل الثاني




تكنولوجيا المعلومات
المخاوف والهموم والمخاطر

تقديم:

هل يستطيع أحد أن يتجاهل التغييرات التي أحدثتها ثورة تكنولوجيا المعلومات في مجتمع المعلومات الحالي؟ بالتأكيد لا يمكن لأحد أن يتجاهل ذلك على الإطلاق، حيث إن هذه الثورة قلبت كثيراً من المعطيات الاجتماعية والسياسية والاقتصادية، بل أحدثت زلزالاً في موازين القوى الاجتماعية وأثرت سلباً وإيجابياً وبالذات الآن على الأوضاع العامة للمجتمعات الصناعية وغير الصناعية (مجتمع المعلومات العالمي) ومن أهم التغيرات التي أحدثتها الثورة المعلوماتية، إنها غيّرت كثيراً في عمق الوضع الاجتماعي والاقتصادي والمهني لأفراد المجتمع لا سيما على صعيد الأسرة.

بيد أن تكنولوجيا المعلومات لم تكن على وفاق تام مع المجتمعات الإنسانية، إذ أن الجانب الإيجابي الذي أغدقته تكنولوجيا المعلومات على المجتمع، رافقه جانب سلبي أثر كثيراً على الترابط الأسري والاجتماعي، بل وحتى على العلاقات الإنسانية، لقد حذرت العديد من المنظمات الإنسانية التي تعنى بشؤون المجتمع بأن هناك خطر حقيقي ناجم عن فوائد التقنية الجديدة والتي قد تكون استغلت من قبل المجرمين في التخطيط والتنفيذ لجرائمهم ولتحقيق مآربهم وأحلامهم غير المشروعة. ولذلك أضافت تكنولوجيا المعلومات هموماً ومخاوفاً، بل وخطراً حقيقياً إضافياً يقع على عاتق البشرية.

١- تكنولوجيا المعلومات والتحدي الاجتماعي:

مما لا شك فيه أن المجتمع البشري يمتاز في عصر العولمة بالانفتاح والتعقيد والتنوع والترابط. كما يمتاز بالتغير الاجتماعي السريع. ولا بد من أن تتأقلم مؤسسات المجتمع مع هذه الخصائص الجديدة. لقد وضعت القمة العالمية لمجتمع المعلومات عدداً من مبادئ المجتمع المعلوماتي وهي: ضمان الوصول للمعلومات للجميع، وتدريب الموظفين بالمهارات اللازمة للانغماس في مجتمع المعلومات، وتأكيد تطوير بنية تحتية معلوماتية آمنة وممكنة وموثوقة على المستوى الوطني مع نفاذ للشبكات الكونية، وبناء وتطبيق استراتيجيات وطنية للمعلومات والاتصالات وتطوير خطط حكومية ملحة لبلدانهم والتحول إلى المجتمع المعلوماتي وتكوين قواعد قانونية، للاستثمار ومحاربة الفساد وحقوق الملكية والنافسة، وحل الصراعات،... الخ، وتطوير التطبيقات اللازمة للاحتياجات المحلية مثل التعليم الإلكتروني، والصحة الإلكترونية، والحكومة الإلكترونية، والتجارة الإلكترونية.

إن التأكيد على الدولة القومية قد ولىّ في عصر العولمة وإن التحكم على المستوى القومي عديم الفاعلية في ظل العمليات الاقتصادية والاجتماعية الكونية. فرأس المال متحرك، حر من أي روابط قومية وهو يستقر حيث تمليه عليه المنافع الاقتصادية، وهناك من يرى أن الدولة القومية قد تحولت إلى سلطات حكم محلي للنظام الكوني. فبالإضافة لما تحمله السيادة الوطنية من معاني الهوية والانتماء والوجود والاستقلال، فهي تحمل معاني تتعلق بمكانة الدولة والمجتمع، والهيبة المحلية والدولية لها، وتحمل جوهر وجودها واستقلاليتها. فالحدود لم تعد كما كانت تمنع وتنتقي الداخل والخارج منها، ولم تعد تعمل كمصفاة للداخلين والخارجين المرغوبين والمطلوبين للدولة أو بين الأصدقاء الأعداء. فهذه الجماعات الأهلية العابرة للحدود مثل أطباء بلا حدود, وجماعة السلام الأخضر وغيرها، وجماعات حقوق الإنسان تجبر الدول على فتح سجونها ومعتقلاتها للتحقيق، وتشترط معونات اقتصادية، وأحياناً تعلق عضويتها في المجالس الدولية الهامة بسجل حقوق الإنسان فيها (١).

إذن وبموجب ما سبق وضعت تكنولوجيا المعلومات المجتمعات الإنسانية أمام تحديات عديدة، من أهمها التحدي الاجتماعي، فهناك اتفاق بين الجميع على مبدأ مهم، وهو أن تكنولوجيا المعلومات قد أطاحت بالحدود بين الدول المتجاورة وغير المتجاورة، مما مهد الطريق أمام العديد من الأعمال أن تنتقل وتجتاز الحدود بدون إذن من الحكومات والسلطات المعنية.

لقد مهدت تكنولوجيا المعلومات للعولمة أن تجتاح أسواق الدول في كل مكان. ففي عصر العولمة هناك عبور للحدود الوطنية للمال، وللتجارة، والمعلومات، والتقنيات، والثقافة، والقيم، والأفكار، والناس، والأمن، والجريمة. ومثلما يؤدي هذا العبور التنمية البشرية والانفتاح والتواصل والانتشار الثقافي والتعاون والمشاركة في جوانب متعددة من الحياة، إلا أنه ليس بلا جانب مظلم، حيث إن زيادة الترابط بين المجتمعات وزيادة الاعتمادية بين مؤسسات المال والأعمال والمنظمات والدول والشعوب والأفراد قد وَلّدَ أنواعاً جديدة من التهديدات الأمنية والاجتماعية. فقد تكونت بنية تحتية افتراضية كونية جلعت مسؤولية حماية الأمن مسؤولية دولية.

على الرغم من محاولات بعض الحكومات في الضبط والتحكم إلا أنها لن تستطيع المحافظة على مجتمعاتها معزولة عن الخارج. إنه من المستحيل منع المعلومات من التدفق عبر حدودها في عصر المعلومات. فلم تعد الحكومات ولا الدول تخشى من بعضها البعض بقدر خشيتها من المنظمات، والجماعات الإرهابية، لا بل إن قدرة الدولة على ضبط الناس، والتحكم بهم قد

أصبحت ضعيفة وستزداد ضعفاً يوماً بعد يوم. إن انتشار الإنترنت في العالم وزيادة حجم المستخدمين لها واستخدامها كآلة لنشر المعلومات ووسيط في التفاعل بين الأفراد والحاسبات دون حسبان للجغرافيا، قد سهل تواصل الأفراد ونقل المعلومات والتقنيات والجريمة والمخدرات عابرة الحدود الوطنية وفي هذا العصر قد حل الدخلاء محل الجنود. وأصبحت ساحات المعارك في كل بيت وشارع وجهاز حاسب ومحطة فضائية وكل موقع على الإنترنت(٢).

لم يتوقف تحدي تكنولوجيا المعلومات للجانب الاجتماعي عند هذا الحد، بل تعداه إلى أكثر من ذلك بكثير، فراحت تكنولوجيا المعلومات تهدد مجتمع المعلومات العالمي في كل برهة من الزمن، وبقدر ما جعلت تكنولوجيا المعلومات العالم يعيش لحظات سعيدة نتيجة ترابطه وتواصله مع بعض، بقدر ما عكرت صفو تلك اللحظات السعيدة نتيجة ارتكاب بعض أفراد هذا المجتمع جرائم أقلقت وزلزلت مضاجع العديد من الناس دون ذنب.

لقد عانت بعض الأسر والمجتمعات البشرية من تحدي تكنولوجيا المعلومات لهم، إذ أن هذه التكنولوجيا قد استُغلت من قبل المجرمين في مجال المخدرات، فهم يستخدمون الإنترنت لتحسين توزيعها وتنظيم إيصال المخدرات للزبائن، وقد مكنتهم من إخفاء المعلومات عن شحنات المخدرات من خلال التشفير عبر الإنترنت. ولقد حددت بعض الدول مثل (انكلترا) عشرات المواقع لبيع المخدرات بما في ذلك (الماروانا)، و(الهيروين)، و(الكوكائين)، وتستخدم عصابات المخدرات مثلاً أدوات تمكنهم من مراقبة من يراقبهم ومن يحقق معهم، ويعترضون الاتصالات ويتجسسون على الشرطة، وكذلك على المنظمات التي تحارب سوء استخدام المخدرات(٣).

يتضح في ضوء مما سبق إن قمة التحدي الاجتماعي الذي توجهه تكنولوجيا المعلومات لمجتمعات اليوم يتمثل في أن مستخدمي هذه التكنولوجيا بدأو يراقبون السلطات، بل ويتجسسون عليها، بدل من أن يراقبواهم من قبل هذه السلطات والحكومات والمنظمات، وهذا الأمر المقلوب زاد من صعوبة وتعقيدات مجتمع المعلومات الحالي، ووفرت تكنولوجيا المعلومات فرصة كبيرة لتشكيل نوع جديد من العصابات والمافيات، وسهل لها عملية الاتصال والتواصل مع بعضها البعض على الرغم من تباعدها مكانياً وزمانياً، وهذا يمثل أكبر تحدي يواجهه مجتمع المعلومات من قبل تكنولوجيا المعلومات ومستخدميها.

٢- تكنولوجيا المعلومات: المخاوف والهموم.

إن المجتمع السعيد هو المجتمع الذي يعيش فيه الفرد في حالة اقتصادية وأمنية واجتماعية وتكنولوجية مرضية ومستقرة، بمعنى آخر، المجتمع السعيد ذلك المجتمع الذي يكون منفلتاً

ومتحرراً من ضغوط الحاجات الاقتصادية، ومتطلباتها، وهمومها وأوجاعها ويحيا فيه الإنسان حالة من الرخاء والوفرة، وعلى الرغم من أن مجتمع المعلومات العالمي الحالي يعيش ويتمتع في نشوة وازدهار وانتصار تكنولوجيا المعلومات، التي جاءت له بالبعيد وقصرت المسافات، وجعلت من الحوار قائماً في الليل والنهار في أرجاء المعمورة من خلال اختزالها للزمن، وفوق وهذا وذاك تأتي المخاوف والهموم والمخاطر التكنولوجية موافقة لحياة وإنسان مجتمع المعلومات العالمي. فمن أعماق هذا المجتمع الذي نراه سعيداً ومحتفلاً ومتباهياً في ذات الوقت بنجاحاته التكنولوجية، ينطلق شقاء جديد وفساد متجدد، ونفس إنساني تصحيه عند الشهيق والزفير المخاطر والمخاوف، من تحول النجاحات التكنولوجية إلى هموم تزحزح حدود الحرية التي طالما حلم بها ردحاً طويلاً من الزمن.

لقد تحولت الفرص الذهبية التي أتاحتها تكنولوجيا المعلومات في مجال التنمية البشرية من حالة الفردوس والنعيم إلى حالة الجحيم، ففي الوقت الذي قادت تكنولوجيا المعلومات الحضارة إلى التحرر إلى حد ما من الفقر والجهل إلى انتصار الفضيلة، وإلى انتصار القيم الإنسانية، وهذا ما سعدت به كثيراً الإنسانية، بيد أن الأمر لم يكن كذلك دائماً، فسرعان ما قامت هذه التكنولوجيا إلى خلق جيل من الأبناء المدللين الذين أفسدتهم نِعم الحضارة التكنولوجية، وقادت هذه التكنولوجيا المتقدمة المجتمع إلى فقر من نوع جديد، ألا وهو فقر الأخلاق الذي بات مجتمع المعلومات العالمي يحيا، ويعيش آهاته وآلامه نتيجة لغياب عنصر الأخلاق والمباديء والقيم التي كانت من أهم معايير المجتمع الإنساني السابق. إن القلق والمخاوف والهموم التي تساور أبناء المجتمع الحالي مشروعة سواء في البلاد المتقدمة والمتخلفة على حدٍ سواء، إذ أن هذه المشكلة تواجه الآن الإنسانية جمعاء في الزمان والمكان المختلفين.

وسط هذه الهموم والمخاوف ينطلق سؤال كبير بكبر حجم الآهات والآلام الإنسانية مفاده، هل هناك ثمن دفعته الإنسانية في عصر تكنولوجيا المعلومات مقابل نجاحاته؟ وهل هناك ثمن دفعناه ومازلنا ندفعه مقابل هذا التقدم المعلوماتي الكبير؟ الإجابة عن ذلك تأتي من قبل الدول التي تمتلك قمة تكنولوجيا المعلومات (الولايات المتحدة الأمريكية) والتي جعلت الإنسانية تقف على كف عفريت أو على شفا حفرة، فهذا رئيس الولايات المتحدة الأمريكية الأسبق جون كيندي يشير في خطابه أمام الأمم المتحدة عام (١٩٦٣) قائلاً: (إننا نملك القدرة لجعل هذا الجيل البشري أفضل الأجيال في تاريخ العالم، أو آخر هذه الأجيال)(٤) ولم يكن هذا القول يتم عصره، بل سبقه قول ابرتراند رسل وتحديداً في عام ١٩٥٢ إذ قال: (نحن على وجه العموم في وسط سباق

بين المهارة البشرية من حيث الوسائل والجنون البشري من حيث الغايات... لقد بقي الجنس البشري في الماضي بنتيجة الجهل والعجز. أما وقد حصلت المعرفة والقدرة مقرنتين بالجنون فلم يعد ثمة ضمان للبقاء)(٥) وأمام هذين القولين لا نملك إلا أن نقول: (إن في العلم نقماً وفي الجهل نعماً أحياناً)(٦).

نضيف للإجابة السابقة إجابة أخرى تخبرنا بما فعلت فينا تكنولوجيا المعلومات، والتي بدلت العديد من الأشياء الجميلة في حياتنا بأشياء تنفث السموم والهموم في حياتنا. فبفعل تكنولوجيا المعلومات استبدلنا حفيف الأشجار، وضرير المياه وتغريد البلابل وزقزقة العصافير وهديل الحمام (هذه الأنشودة الموسيقة الأزلية) بهدير الطائرات وأبواق السيارات والأغنيات الهابطة، واستبدلنا عبق الأزهار بعوادم السيارات وحرقنا الغابات وقطعنا الأشجار، لنشيد بدلاً عنها كتلاً من الأسمنت التي تنفث السموم من مداخنها عوضاً عن قارورة العطر التي كانت تفوح منها بيوتنا القديمة، فأينما نولي وجوهنا هناك تلوث بالبيئة، وتلوث يؤذي العيون، ويؤذي الأسماع، وتلوث يؤذي الروح والنفس وحتى القلوب (٧).

بيد أن اللافت للنظر أن رؤية المجتمع لنقمة وهموم ومخاوف ثورة تكنولوجيا المعلومات لم تفق عند هذا الحد، بل راحت وراءهم إلى أبعد من ذلك بكثير. والحق أكل الحق معهم بكل تأكيد، ويأتي هذا التأكيد لتلك التصورات والرؤى لكونها نابعة من أرض الواقع، ويمكن أن نضع بعضاً من الآثار السلبية لتكنولوجيا المعلومات في المجتمع أمام القارئ الكريم، حيث يرى البعض أن التزايد المعرفي والمعلوماتي لم تصاحبه مساواة اجتماعية ومعرفية سواء داخل الدولة الواحدة أو بين الدول، فقد خلق فجوة معرفية بين الدول والفئات الاجتماعية، حتى قيل إن العالم مهدد بنوع من الأبرتهايد المعلوماتي، فهناك المنتفعون بقوة المعلومات، وهنا الأميون في هذا المجال المعرضون للتهميش بسبب عدم توافر البناء التحتي اللازم لإلحاقهم بهذه الثورة مع انتشار ما يسمى بالواقع الإفتراضي (Virtual Reality)، أي واقع هو من صنع الخيال، ولا أساس لوجوده في الواقع الحقيقي، فبوسع المنتفعين بهذه الثورة أن يتلاعبوا مع الصور، وبالتالي مع الحقائق، وأن يصطنعوا صوراً للواقع لا وجود له، مما يمكنهم من التلاعب بمقدرات عالم المهمشين الأميين الملفوظين من عالم ثورة المعلومات، وهذا أمر من شأنه الإساءة أخلاقياً وأدبياً وحضارياً إلى المنتفعين بهذه الثورة، وإلى المهمشين العاجزين عن مواكبتها على حدٍ سواء.

فوق هذا وذاك، وما يدعو للدهشة حقاً، وما يذعر إنسان مجتمع المعلومات العالمي في ذات الآن، إن قائمة الهموم والمخاوف والسلبيات المتعلقة بتكنولوجيا المعلومات أخذت بالازدياد، بل

والاستمرار، ويضاف إلى ما سبق، أو ثورة المعلومات لم تؤد إلى تحقيق نوعية جيدة من الحياة للبشر، فهي تسرّع من خطى الحياة بشكل يجعل المرء يلهث وراءها، من دون جدوى حقيقية، كما قلصت من الوقت المتوافر لهم لكي يستمتعوا بها ويتفقهوا في كنهها. كذلك يمكن القول: إن تكنولوجيا المعلومات تدخلت بشؤون أفراد المجتمع تدخلاً مريباً، بل وسافراً من حيث إنها جردت الفرد من خصوصيته الخاصة، إذ أن ثورة المعلومات تقضي على خصوصية الأفراد وحقهم في الحفاظ على حرماتهم وأسرارهم الخاصة، فقواعد المعلومات المرتبط بعضها البعض، والتي تحتوي إلى أسماء الأفراد وعناوينهم ووظائفهم وحالتهم الاجتماعية والصحية بل ونوعية مشترياتهم - عن طريق التزايد في استخدام الكروت الإئتمانية والممغنطة وغيرها - ممّا يهدد مستقبلهم، وقد يعرضهم لمخاطر لم تكن في حساباتهم، ومن المتوقع أن تزداد قدرة الآخرين على رصد تحركاتنا، بل إن إحدى الشركات الأمريكية أعلنت أخيراً استعدادها لإطلاق قمر اصطناعي للتجسس الشخصي، حيث يمكن للفرد العادي دفع مقابل مالي معين ليرصد تحركات ومواقع شخص آخر. كما أن ثورة المعلومات تغزو من ناحية أخرى خصوصية ثقافة المجتمعات، وتهدد ذاتيتها الثقافية، وهي مشكلة ليس لها حل سوى العمل على التقليل من آثارها(٨).

يواصل الفريق الذي يرى أن تكنولوجيا المعلومات تمثل شبحاً مخيفاً للإنسانية الساعية إلى التخلص من عالم القتل والدمار والفساد، يواصلون توجيه انتقاداتهم لتكنولوجيا المعلومات مظهرين بصحمة الآثار السلبية التي تركتها هذه التكنولوجيا في المجتمع، يرى هؤلاء أن ثورة المعلومات لم تحقق شيئاً يذكر لدعم الديمقراطية، على الأقل حتى الآن، فبالرغم من الوعود بدعم عمليات المشاركة الجماهيرية من خلال الوسائل الإلكترونية التي تحقق الفورية والتفاعلية والحوارية، وما يقال عن الاجتماعات الإلكترونية للمدينة أو القرية من خلال شبكات الاتصال، لم يحدث شيء ذو بال حتى الآن، وتشير الاستطلاعات التي أجريت في بعض المجتمعات التي يطلق عليها مجتمعات المعلومات، إلى أن (٣٣%) من المراهقين لم يكن بمقدروهم تحديد أسماء ممثليهم في المجالس التشريعية، حتى قيل إنه كلما زاد المجتمع تعقيداً، ابتعد الناس أكثر عن السياسة وفضلوا عليها الترفيه الإلكتروني.

يبقى تسجيل الآثار السلبية لتكنولوجيا المعلومات مستمراً، ولم تقف هذه الآثار عند حدود الإنسان فقط، بل طالت حتى الطبيعة، لقد أشارات العديد من الدراسات إلى أن تكنولوجيا المعلومات هي تكنولوجيا نظيفة وودودة وغير ملوثة، إلا أن واقع الحال لم يكن فيه كل هذا الكمال الذي وعدتنا فيه الدراسات التي حدثتنا عن تكنولوجيا المعلومات، إن ثورة المعلومات

ألحقت تدميراً فادحاً بموارد البيئة الطبيعة، ليس أقلها ما تحدثه صناعة الكمبيوترات من ملوثات، كما أنه على النقيض من القول بأن الإلكترونيات سوف تقلل من الورق، فإن الطلب على الورق يزداد.

عندما صُنعت تكنولوجيا المعلومات وبدأت تطبيقاتها فوق أرض الواقع، وباتت تلازم الإنسان أينما حل وارتحل وهي فعلاً كذلك وأصبحت صديقاً ورفيقاً ملازماً للإنسان، إلا أنها مع مرور الزمن نقضت العديد من وعودها وتملصت من صداقتها للإنسان، وفي كثير من الأحيان اصبحت عدواً له، وليس رفيقاً وصديقاً، وتمثلت حالة العداء من حيث أنها أقالته من وظيفته، إذ أن ثورة المعلومات قلصت كم الوظائف المتاحة، ومن المتوقع أن يزداد هذه التقلص في المستقبل، مع إحلال الإنسان الآلي والكمبيوتر محل الكثير من الوظائف، فمنذ عام (١٩٧٨) فقد (٤٣) مليون فرد وظائفهم في أمريكا، كما تغير مفهوم الوظيفة التي تستمر مدى حياة الفرد، وحتى في بعض الوظائف التي يشعر البعض بأنها آمنة فإنه يوجد ما يسمى (خبير أنظمة) وعمله يتمثل في الحد من الوظائف، ومن ناحية أخرى خلقت الثورة المعلومات ما يسمى بالاقتصاد الاصطناعي.

بعد كل ذلك يستوقفنا سؤال مهم مفاده: ترى هل توقفت الآثار السلبية لتكنولوجيا المعلومات عند هذا الحد؟ أم أنها أخذت خطيرة وعميقة ضربت في أعماق المجتمع؟ إن ثورة المعلومات تمثل تهديداً للأمن القومي للمجتمعات، فمثلما نستطيع أن نشن حروباً معلوماتية وحملات دعائية، فإننا في ذات الوقت عرضة لمثل هذه النوعية من الحروب والإرهاب المعلوماتي، بفعل السنوات المعرفية والمعلوماتية المفتوحة، والعولمة التلفازية. فقد أصبح العالم قرية صغيرة تكاد معلوماتها تكون على المشاع ما لم تتوافر إمكانات فاعلة لصيانتها من الاختراق (٩).

سعت المجتمعات الإنسانية من وراء استخدامها لتكنولوجيا المعلومات في مرافق الحياة المختلفة، لخلق مجتمع جديد خالٍ قدر الإمكان من الجرائم والسرقات، إلا أن هذا لم يتم، فأصبحت تكنولوجيا المعلومات في العديد من الأحوال معول هدم وتدمير لبنية المجتمع، فأخترقت القوانين ليس تحت جنح الظلام، بل في وسط النهار، لكن دون أن يراك الآخرون، ماذا تفعل وأنت تجلس سواء في بيتك أم في مقاهي الإنترنت، حيث إن ثورة المعلومات قد أتت بآثار سيئة على النظام والقانون، فجرائم الكمبيوتر تلحق خسائر فادحة بأصحاب الأعمال والحكومة، كما زادت ظاهرة التجسس التجاري والاقتصادي بين الشركات والدول، ففي فترة زمنية قريبة مضت نشأت مشكلة بين الولايات المتحدة وكندا من جانب والصين من جانب آخر عندما قامت الأخيرة

بنقل تكنولوجيا لصناعة الإلكترونيات وأشرطة التسجيل وصنعتها لتبيعها في أسواق هاتين الدولتين بثلث أسعار منتجاتها المماثلة، ومع زيادة المنافسة العالمية ستزداد دوافع التجسس التجاري حدة بعد بدء تنفيذ الاتفاقية العامة للتعرفة والتجارة (الجات) واكتمال آليات تنفيذها بالنسبة للدول النامية. وبخصوص المستقبل، فإن بعض المتابعين والراصدين للآثار السلبية لتكنولوجيا المعلومات، يرون أن المستقبل ضبابي، مشوش، بل وإن إمكانية التنبأ به تكاد تكون عملية صعبة. حيث إن ثورة المعلومات تلقي بظلال كئيبة على المستقبل، فالواقع الراهن يشير إلى تراجع في (كم وكيف) التفكير المستقبلي، حيث قللت هذه الثورة من إثارة المستقبل وعجائبه، وجعلت من الصعوبة التنبؤ بصور المستقبل، أو التفكير فيه بطريقة منظمة. وأفرزت نوعيات من البشر تريد أن تخرج من حلقة الدروان السريع للحياة.

إن أهم جانب سلبي لثورة المعلومات هو أن وفرة المعلومات قد يضر برؤوس البشر، لقد أطلقت تكنولوجيا المعلومات الشرارة لإشعال فتيل ثورة المعلومات الكبرى، بل يمكن القول: إن اعصار المعلومات الجارف أحدث زلزالاً مدوياً في عقول الإنسانية، والأسئلة المهمة هنا تطرح نفسها بشكل تلقائي ومفادها: هل سيعصف هذا الإعصار بعقل الإنسان؟ وهل سيصاب بتخمة المعلومات ليسحق منهزماً أمامها؟ أم أن الإنسان يكتفي منها بالقشور والمرور العابر؟ أم أن الإنسان سيلوذ بقوقعه تخصصه؟ هل سيستكين أم سيتصدى العقل الإنساني الوثاب لهذا التحدي الجديد مجدداً معارفه ومهاراته وأدواته يروض بها مارد المعلومات الذي انطلق من عقاله؟

لقد كانت في السابق المشكلة تتجسد في ندرة المعلومات أو الشح المعلوماتي (Under – information)، أم الآن، فقد انقلب الوضع تماماً إلى نقيضه لتصبح المشكلة هي الإفراط المعلوماتي (Over – information) أو حمل المعلومات الزائد كما يطلق عليه البعض، وهي مشكلة لا تقل صعوبة عن سابقتها إن لم تكن أكثر حدة وإثارة، إن المعلومات تتضاعف بمعدل هندسي، حيث تنتج البشرية حالياً من المعلومات والمعارف في سنوات قلائل قدراً يفوق ما كانت تنتجه سابقاً في قرون (١٠) وهذه الزيادة المفرطة تنتج عنها تخمة معرفية ومعلوماتية، وهي ليست مشكلة إحصائية، فقد قدرت موسوعة المستقبل (Encyclopedia of the future) أن المعلومات العلمية المتاحة للبشر تتضاعف كل (١٢) سنة، وأن المعلومات العامة تتضاعف كل سنتين ونصف السنة، وهو ما يعني وجود تراكم معلوماتي ومصرفي، يفرز ضغوطاً نفسية وعصبية، مما يقلل في المقابل من الإنتاجية في العمل، ومن التركيز في أماكن الدراسة والبحث، كما يلاحظ أن التخمة المعلوماتية المتوافرة هي أقرب للترفيه والاستغلال التجاري منها إلى

المعلومات المفيدة التي تقود حركة المجتمع والأفراد، كما قللت هذه التخمة من القيمة الذاتية للمعلومة في عصر يغلب على ثقافته قلة الحاسة النقدية والتحليلية والمعارضة والميل إلى التوفيقية.

أضف على ما سبق، أن الحكومات هي الأخرى تشارك أفراد المجتمع من حيث الرؤية لنقمة ثورة تكنولوجيا المعلومات، فهي الأخرى طالتها سلبيات تكنولوجيا المعلومات، حيث إن ثورة المعلومات وما أفرزته من سرعة في نشر الأخبار بُشكل أحد الجوانب السلبية من وجهة نظر الحكومات، فقد أدى التطور الكبير في وسائل الاتصال إلى جعل الناس يعرفون الأخبار الجديدة بسرعة شديدة، لاسيما أخبار الأزمات الخطيرة أو الموضوعات ذات الحساسية، ويؤدي ذلك إلى ممارسة ضغوط على الحكومة من أجل سرعة حل هذه الأزمات في حين يحتاج المسؤولون الحكوميون إلى وقت كاف لدراسة هذه المشكلات، ووضع البدائل والتخطيط، وكانت الحكومات في السابق تتخذ قراراتها من دون ضغوط من الرأي العام، نتيجة بطء معرفة الرأي العام للأخبار ذات الحساسية العالية، وبالتالي باتت الحكومات في ظل ثورة تكنولوجيا المعلومات على أهبة الاستعداد لمواجهة الشعوب، وربما لمواجهة مصيرها نحو الزوال إذا لم تكون عاملة بصدق وصادقة في ذات الآن مع شعوبها.

اللافت للنظر في ثورة تكنولوجيا المعلومات إنها سهلت عملية السطو على حقوق الآخرين أثناء الليل والنهار، وأمام الملايين من البشر، وعلى مرأى ومسمع من الحكومات، إذ أن ثورة المعلومات قد زادت وضعية قضية حقوق النشر سوءًا، فقد أتاحت الأقمار الصناعية ونظم الكابل إمكان التقاط برامج التلفاز من محطات أخرى تبعد آلاف الأميال، وتسجيل هذه البرامج، وبيعها من دون موافقة، كذلك انتشرت آلات التصوير التي تطبع آلاف النسخ من الكتب دون الحصول على موافقة المؤلف أو الناشر على حقوق النشر، وينطبق نفس الشيء على برامج الراديو والتلفاز وأفلام السينما مما يهدد نظام حق النشر، وحماية المؤلفين (١١).

تأتي المخاوف والهموم أيضاً من تكنولوجيا المعلومات من خلال ما يسمى بأمراض الحاسوب والإنترنت، فلقد أثبتت الدراسات أن حالات الاجهاد البصري (Eye strain) تزداد بنسبة (٥٥%) لدى مستخدمي الحاسوب مقارنة بنظرائهم مستخدمي الآلة الكاتبة العادية.

نظراً لأن شاشة الكمبيوتر تعمل بنفس طريقة شاشة التلفاز، فإن الضوء المنبعث منها يبث معه إشعاعاً قد يضر بمستخدمي الحاسوب الذي يقترب من هذه الشاشة بمسافة أقل من قدمين

(٦٢سم)، وتزداد خطورة مشاكل الإشعاع خاصة لدى السيدات عند استخدام الحاسوب في فترات العمل، فقد ينتج عنه وجود تشوهات خلقية بالجنين أو سقوطه في بعض الأحيان.

تؤكد مصادر المعلومات أن أمراض الحاسوب متعددة ومنها أيضاً ما يصيب العين بالمياه الزرقاء، إذ ينتج عن الإشعاع الصادر عن الحاسوب أيضاً إصابة العين بالمياه الزرقاء، ولذلك فإن على المستخدم الحذر لا سيما عند استخدام الشاشات الملونة؛ لأنها أكثر اتساعاً من الشاشات العادية (الأبيض والأسود) مما أدى استخدام الطابعات المرافقة للحاسوب إلى زيادة مستوى الضوضاء في أماكن العمل، وبالرغم من تعوّد الموظفين على أصوات الطابعات مع مرور الوقت، فإن الضوضاء الصادرة عن تلك الطابعات بشكل متواتر وثابت، لاسيما تلك التي تصدر صوتاً أثناء الطباعة المعروفة باسم (Impactprinters) قد يترتب عليها ارتفاع ضغط الدم لشعور الفرد بالضيق والتوتر العصبي أحياناً، هذا فضلاً عن عدم قدرته على التركيز الذهني، وصعوبة قيامه بأداء بعض العمليات التي تتطلب الدقة كالعمليات الحسابية مثلاً. وقد حددت إدارة السلامة والأمن الصناعي في الولايات المتحدة الأمريكية معدلات الضوضاء (مقاسة بالديسيبل) وطبقاً لهذه المعدلات فإن الحد الأقصى لمعدل الضوضاء المسموح به في مكان العمل هو (١١٥) ديسيبل.(١٢)

علاوة على ما سبق، قد ينشأ عن الجلوس أمام الحاسوب لمدة طويلة وبشكل مستمر يومياً تقوس في الظهر وآلام في الرقبة والأكتاف، وبالرغم من أن هذه المشكلات يعود البعض منها إلى عصر ما قبل الحاسوب فيما يعرف بمتلازمة السكرتارية (secretary syndrome) والتي تظهر أعراضها في تصلب الرقبة واقتراب الأكتاف من بعضها ووجود آلام في الذراعين والعمود الفقري، فإن هذه الأعراض قد ازدادت مع انتشار الحاسوب، وتزداد آثار هذه المشكلات مع الجلوس غير المريح أمام الحاسوب والذي قد يؤدي إلى الحد من تدفق الدم إلى أجزاء الجسم ووجود الدوالي في الأرجل وغيرها.

قد يدهش البعض إذا علم أن استخدام الحاسوب في أماكن العمل قد أدى إلى وجود بعض المشكلات النفسية التي اقترنت باسم الحاسوب مثل الخوف من أو كراهية الحاسوب (computer phobia) ومتلازمة الحاسوب (computer syndrome)، ويشير الأول إلى حالة نفسية تعني خوف الفرد من الاقتراب من الحاسوب أو استعماله، وقد أثبتت الدراسات أن هذا المرض لا يترتب بالسن أو النوع أو درجة التعليم أو الظروف الاقتصادية للفرد، وقد ينشأ المرض نتيجة الخوف من المجهود كما يقولون، وينتج عن وجود قلق يترتب عليه وجود ضغط وشد نفسي

وعضلي ووجود أعراض أخرى مثل الصداع وغيره، ويرى البعض أن الخوف من الحاسوب يهدد الكينونة أو الذاتية الشخصية، فالعمل الذي كان يحتاج إلى خبرة الفرد ولمساته الشخصية أصبح يؤدي الآن وبشكل أسرع من خلال صندوق إلكتروني (الحاسوب)، وهذا الأمر يفقد الفرد سيطرته على عمله وشعوره بالإنجاز الشخصي أو الذاتي، هذا جزء من ثمن التقدم الذي تعيشه البشرية الآن.

أما متلازمة الحاسوب (computer syndrome) والذي نشر عنه أخيراً فإنه يختلف عن مرض الخوف من الحاسوب، حيث أن ملازمة الحاسوب تعود إلى الإجهاد والتوتر النفسي من جراء متابعة النقاط المنبعثة على الشاشة وليس بسبب الإشعاع، كما أنه يعود إلى إدمان الأفراد لملاحظة شاشات الكمبيوتر والذي قد يترتب عليه زيادة في هرمونات التوتر، وهذه الزيادة تؤدي إلى الشعور بسخونة وحكة في الجلد، وتختفي هذه الأعراض بمجرد التوقف عن العمل على الحاسوب، ولذلك ينصح الخبراء بعدم الجلوس أمام الحاسوب لفترات طويلة تفادياً لمثل هذه الأمور.

هناك أيضاً ما يسمى بالانطواء على الحاسوب أو انطوائية الكمبيوتر (computer bhylliac)، وتوجد هذه الحالة عندما يستغرق الحاسوب على الشخص وقته فيستمر في العمل عليه بشكل يشبه مدمني المقارن، وقد توجد هذه الحالة لدى الأفراد الانعزاليين ذوي الشخصيات الانطوائية أو الأشخاص الذين يرغبون في الهروب من ظروفهم ومشكلاتهم الحياتية فيلجأون للحاسوب ليفرغوا فيه همومهم، وقد أطلق البعض على هذا المرض لفظ متلازمة السيليكون (silicon syndrome) في إشارة إلى الحاسوب. (١٣)

٣- تكنولوجيا المعلومات تدق ناقوس الخطر:

في ظل ثورة تكنولوجيا المعلومات التي تكاد تكون اجتاحت كل أركان المجتمع، لا يمكن الحديث عن العولمة بمعزل عن تكنولوجيا المعلومات، والعكس صحيح أيضاً، فالأخيرة هي السفينة التي ركبتها العولمة وطافت بها أرجاء العالم، وهنا عندما نتحدث عن العولمة وسلبياتها فإننا في الوقت ذاته نكشف النقاب، بل ونميط اللثام عن المخاوف والمخاطر الحقيقية التي تحدثها تكنولوجيا المعلومات في المجتمع، لقد أضحت تكنولوجيا المعلومات واقعاً ملموساً لا نستطيع الهروب أو الفرار منه، بل يتطلب الأمر التعامل معه، وعلى الجميع حكاماً وشعوباً، تقع مسؤولية التململ والتعايش والعيش في ظل هذا الواقع بحلوه ومره، وأن نتجرع من كلا الكأسين، وأن نستسيغ الطعم الجديد، محاولين أن نتجنب قدر الإمكان الجانب السلبي (المر) منه، وهذا بطبيعة

الحال متروك لنا ولقدرتنا وإمكانياتنا المتاحة والكامنة منها، ويجب أن ننظر بعمق إلى طبيعة الدور الإيجابي والفرص التي تمنحها تكنولوجيا المعلومات، محاولين قدر الإمكان التقليل من الأثار السلبية التي تتركها هذه التكنولوجيا في المجتمع.

لقد أصبحت تكنولوجيا المعلومات اليوم ذات أثر كبير في المجتمع، من الناحية الإيجابية والسلبية معاً، وإذا كان الجانب الإيجابي فيما مضى يدعونا إلى أن نغض النظر أو نحجبه عن سلبيات تكنولوجيا المعلومات، فإن الأمر اليوم وبعد أن تغلغلت في أعماق المجتمع وباتت كأنها الرئة الجديدة التي يتنفس عبرها إنسان مجتمع المعلومات العالمي، فإن الأمر يجبرنا ألا نغض النظر عن الجانب السلبي في ظل المعطيات الراهنة التي تعيشها الإنسانية، والسؤال المهم هنا مفادهُ: أين يكمن خطر تكنولوجيا المعلومات؟ وكيف دقت تكنولوجيا المعلومات ناقوس الخطر في مجتمع المعلومات العالمي؟

لقد صدق من قال: إن المجتمع لا تشكلّه السياسة أو الاقتصاد، بقدر ما يشكلّه نظام التواصل السائد بين الأفراد والجماعات والمؤسسات، وقد جاءت تكنولوجيا المعلومات لتزيد هذا المفهوم رسوخاً، ودعنا نلهو قليلاً برصانة الأوصاف التي ما فتئوا يخلعونها على هذا الإنسان الضائع، الحائر بين عصور الأحجار والمعادن والمداخن والمفاعلات والمعلومات فالإنسان بناء على المفهوم الحالي- ليس هو الهوموبوليتك (الإنس- سياسي) ولا هو الهوموإيكونوميك (الإنس - اقتصادي) بل هو في حقيقة أمره الهموكومنيكيك (الإنس - اقصالي). ما قصدته بلهو (الهمو- تيك) هو أن ألفت الأنظار إلى مدى الخطورة التي تنطوي عليها تبعية الإنسان للتكنولوجيا، وليس العكس.(١٤)

بناءً على ما سبق فإن تكنولوجيا المعلومات عززت التواصل بين المجتمعات الإنسانية، ويتضح هذا التعزيز والتواصل من خلال تعزيز هذا النوع من التكنولوجيا لظاهرة العولمة، ومن هنا تبدأ ملامح خطورة تكنولوجيا المعلومات بالظهور شيئاً فشيئاً، فمن أجل أن نقترب من صياغة تعريف شامل للعولمة، فلا بد من ان نضع في الاعتبار ثلاث عمليات تكشف عن جوهرها:

العملية الأولى: تتعلق بانتشار المعلومات، بحيث تصبح مشاعة لدى جميع الناس. أما العملية الثانية: فتتعلق بتذويب الحدود بين الدول. وأما العملية الثالثة: فهي زيادة معدلات التشابه بين الجماعات والمجتمعات والمؤسسات، وكل هذه العمليات قد تؤدي إلى نتائج سلبية بالنسبة إلى بعض المجتمعات، وإلى نتائج إيجابية بالنسبة إلى بعضها الآخر. وأياً كان الأمر، يمكن القول: إن

جوهر عملية العولمة يتمثل في سهولة حركة الناس والمعلومات والسلع بين الدول على النطاق الكوني (وكل تلك العمليات جسدتها تكنولوجيا المعلومات فوق أرض الواقع بكل جوانبها المتعلقة بها).

إن خطر عملية العولمة التي تحققت أهدافها من خلال تكنولوجيا المعلومات، يكمن في عملية الصراع المستمر بين العولمة والمحلية، فالعولمة تقلل من أهمية الحدود، بينما تؤكد المحلية على الخطوط الفاصلة بين الحدود، والعولمة تعني توسيع الحدود، في حين أن المحلية تعني تعميق (تضييق) الحدود. وفي المجال الثقافي والاجتماعي، تعني العولمة انتقالاً للأفكار والمبادئ وغيرها، بينما المحلية قد تميل في بعض الأحيان إلى منع انتقال الأفكار والمبادئ.(١٥)

يظهر خطر تكنولوجيا المعلومات من خلال العولمة الاتصالية، فهناك عولمة اتصالية تبرز من خلال البث التلفازي عن طريق الأقمار الصناعية، وبصورة أكثر عمقاً من خلال شبكة الإنترنت التي تربط البشر في كل أنحاء المعمورة، وتدور حول الإنترنت أسئلة كبرى، ولكن من المؤكد أن نشأتها وذيوعها وانتشارها أمور ستؤدي إلى أكبر ثورة معرفية في تاريخ الإنسان. لقد أثار مارشال ماكلوهان، واضع الصيغة الشهيرة (القرية الكوفية)، جدلاً في الستينات لاعتقاده أن الحياة الخاصة والمذهب الفردي مهدّان بفعل التطور التقني في مجال الاتصالات، كان ماكلوهان يقول: إن الكهرباء هي قوة قادرة على جمع شعوب القادة كلها في القرية الكونية، فالكهرباء لا تصطدم بأي عائق سياسي أو جغرافي، فهي تجتاز الحدود وتقطع القارات والمحيطات في لحظة ومن دون عقبة، وهكذا فهي تقرب بين الأشخاص والأشياء.(١٦)

تواصلاً مع ما سبق، وعلى الرغم من أن الليبرالية الجديدة كانت القوة الدافعة وراء العولمة، فإن بعض نتائج تلك العولمة لم تكن مرغوبة أو متوقعة من قبل من روجوا لها وما أكثرهم. وما أكثر ما طرح السؤال الأساسي: هل العولمة دين الحداثة أم نذير نهايتها؟ وإلى أين يذهب بنا هذا الاقتصاد العولمي معصوب العينين الذي جعل من مصير البشر لعبة تتقاذفها أياديه الخفية وتقلبات أسواقه وقصر خطر إستراتيجياته وتكتيكاته؟ أليس من الجائز ألا يكون هناك إياد خفية أصلاً، وما هي إلا لعبة من ألعاب اللغة التي تعمل في سراديب اللاوعي الاجتماعي لإخفاء القوى السياسية-الاقتصادية الكامنة وراءها؟ فمن وجهة نظر جون جراي، ما هذه الأيدي الخفية إلا وسيلة لإخفاء يد السلطة التي صنعتها، سلطة الداخل متضافرة مع مصادر السلطة خارجها. فكيف لنا أن نفسر هذا التناقض الحاد بين هذا النمو الاقتصادي الهائل (إجمالي الناتج العالمي

٣٣ ألف مليار دولار سنوياً) وتزايد عدد الفقراء وطوابير البطالة وانتشار المجاعات؟ وفوق هـذا وقبـل ذاك، كيـف أدى هذا الاقتصاد إلى بؤس الإنسان واغترابه؟ بدلاً من رفاهية هذا الإنسان، غاية الاقتصاد في الأسـاس. إن أخطـر أسـباب اغتراب عمالة العصر هو نزعة سـحق المهـارات، أي تفكيكهـا إلى مهـارات أصـغر فأصـغر ليـتلاشى، مـع عمليـة التفكيـك الدؤوبة تلك ، الطابع الشخصي للمهارات الإنسانية. ولا شـك في أن تكنولوجيـا المعلومـات تلعـب دوراً حاسـماً في الإسراع بعملية تفكيك المهارات تلك. ولا غرابة في هذه النزعة التفكيكيـة لتكنولوجيـا المعلومـات، فهـل لنـا أن ننـسى أن جميـع المشكلات يتم (تفكيكها" معلوماتياً في نهاية الأمـر إلى ذرات "الـصفر والواحـد" في حـين يعـرف بعـض علـماء الكمبيـوتر عملية الذكاء الاصطناعي بأنها تلك العملية التي نظل من خلالها نفتت ونفتت حتى لا يبقى هناك ذكاء.

هكذا أطاحت تكنولوجيا المعلومات وأتمتتها بفرص العمل، "وهذا الخطر الأكبر بعينه" وأصبح العـالم ، شـأنه وشـأن قطع الغيار، يمكن استبدال غيره به من أصحاب الياقات الزرقاء أو من أصحاب الياقات المعدنية مـن فـصيل الروبوتـات، لقد اكتملت فصول تراجيديا العمالة الإنسانية على مرأى ومسمع من الجميع، بعـد ان تـم اسـتقطاب المهـارة إلى أعـلى، وقد احتكرها أصحاب الياقات البيـضاء مـن نخبـة التكنـوقراط المـدجبحين بـنظم المعلومـات مـن مخططـين ومـصممين ومحللين اقتصاديين ومسوقين محليين وإقليميين وعالميين، وعلى ما يبدو فإن عهدنا بالتكنولوجيا كما قال قائل: أن تنحـاز إلى صف الكبير على حساب الصغير.(١٧).

زد على ذلك إن خطر تكنولوجيا المعلومات أُخذ من خلال العولمة الغرب العديد من المصالح الاجتماعية، بل ضارب سيادات الدول ذاتها. لقد حذر الكثيرون من المصير المشؤوم الـذي تـدفع العولمـة إليـه دول الأطـراف، فهـي تقلـص مـن سلطات هذه الدول وتضيق الخناق على مناورتها، وهكذا تظـل سـيادتها تتآكـل إلى أن تـصبح هـذه الـدول عـاجزة عـن الوفاء بالتزامات العقد الاجتماعي تجاه مواطنيها، يحدث هذا تدريجياً ولكن بصورة متسارعة، لتجد تلـك الـدول نفـسها وقد تحولت من راعية لمصالح هؤلاء المواطنين إلى حارسة لليبرالية السوق الجديدة، حامية لرأس المال الخارجي والمحلي.

حالما يشتد عود العولمة حتى تجد الحكومات المحلية نفسها أضعف من أن تفي بواجباتهـا الاجتماعيـة كالتأمينـات الاجتماعية والخدمات التعليمية والرعاية الصحية وحماية البيئة وما شابه. ولا يقف الأمر عند هذا الحد، بل تصبح هذه الحكومات المحلية عاجزة أيضاً عن تقديم العون

لرأس المال العالمي فيما يخص تأمين حقوق الملكية بأنواعها، والحفاظ على الأمن الاجتماعي، وحماية الاستثمارات ضد الجريمة المنظمة وضد ردود أفعال المقهورين وهنا تشيح المؤسسات المتعدية الجنسية بوجهها عن الحكومات، لتستدير صوب المنظمات الدولية طالبة دعمها، دعماً يخترق الحدود وينتهك السيادات ويهزأ بالنظم المحلية والهويات القومية، ويتنامى الشعور بإمكان حكم الدول من خلال تلك المنظمات الدولية، ويزداد سخط الشعوب على حكوماتها بالتالي، والتي لا تجد مخرجاً لتبرير عجزها إلى التعلل بضرورة الخضوع لقوانين المنافسة الأجنبية وفتح الأسواق المحلية على مصاريعها، وهكذا تتوالى خسائر العولمة، خسارة اجتماعية في تبخر فرص العمل ومزيد من الاختلال في توزيع الدخول والثروات، وخسارة أخلاقية من أبرز مظاهرها تحقيق الثروات بطرق غير مشروعة وتقويض العلاقات الأسرية، وخسارة أمنية في نمو جرائم الكبار بدافع الجشع ، وجرائم الصغار بدافع غريزة حب البقاء، وخسارة بيئية في استنزاف الموارد الطبيعية وانتشار الملوثات بما فيها تلك التي بدأ تأثيرها يظهر على مظاهر الرجولة أو ما يعرف بظاهرة (تأنيث الطبيعة) ولا تكتمل قائمة الخسائر دون ذكر للخسارة الثقافية من تسطيح الثقافة وابتذالها وطرد الثقافة الرديئة للثقافة الجيدة، ناهيك عن الرفيعة، إن العولمة، كما توقع الكثيرون، لن تؤدي في العالم النامي إلى تهميش الأقليات فقط، بل إلى تهميش الأغلبية أيضاً.(١٨)

فرح الناس كثيراً بالوعود التي قطعها أصحاب العلم والمعرفة (التكنوقراط) على أنفسهم، عندما وعدوا المجتمع الإنساني بفردوس أرضي، طالما أن تكنولوجيا المعلومات أخذت بالتقدم اللامحدود، فهي نبع لا ينضب من بدائل الحلول ومصادر الطاقة المتجددة، ومواد جديدة تعوض ما أهدرنا من مواد طبيعية، ووسائل عدة توفر الراحة والرفاهية، والغذاء والكساء والمسكن، وتعلم الصغار وتؤهل الكبار، وتشفي العلل وتطيل الأعمار، أما عن آثار التكنولوجيا السلبية وخرائبها البيئية ومآسيها الاجتماعية وأضرارها النفسية، فيوصي هؤلاء التكنوقراط بأن يهدأ الجميع بالاً، فحل مشكلات التكنولوجيا هو مزيد من التكنولوجيا.

بيد ان النجاح التكنولوجي الذي تحقق في مجال تكنولوجيا المعلومات كان له ثمناً كبيراً دفعته، وما زالت تدفعه الإنسانية، إن قمة نجاح تكنولوجيا المعلومات يقابله خطر حقيقي يهاجمنا في أعماق نفوسنا، إنه الخواء الروحي الذي بدأت تعيشه البشرية، ففي الوقت الذي بدا لنا الكون وكأنه خاضع لفكرنا، تقوده إرادتنا لغايات محددة، واسترخينا تحت وهمٍ يصوّر لنا العلم والتكنولوجيا قوة طوع أيدينا وتحت سيطرتنا، وماله من وهمٍ ساذج ، فليس لنا اليوم حياة مستقلة

بمنأى عن سيطرة هذه التكنولوجيا الآسرة، وربما يكون العكس أقرب إلى الصواب، فقد أوشكت التكنولوجيا، في غمرة نجاحها، أن تستقل بذاتها، تفرض علينا منطقها وقيودها، لقد قامت حياتنا المادية على تكنولوجيا غاية في النجاح، في حين تئن حياتنا الروحية تحت وطأة الخواء، فقد ألهتنا هذه التكنولوجيا بقدرتها الفائقة على إحداث التغيير، فنسينا ما بقي وسيبقى دوماً ثابتاً بداخلنا دون تغيير، لقد نسينا مطالبنا الوجدانية، وحاجتنا الدائمة إلى المثل العليا وإلى الألفة والتآخي والإحساس بالذات وبالهوية. ومع المد العلمي والتكنولوجي، انحسر الخطاب الديني، ومضى غلاة العقلانيين في غيهم وفي أحادية نظرتهم، يعلنون أن الدين ظاهرة عقلانية، مآلها إلى الاندثار حتماً في مجتمع انتصار العقل والحسم العلمي ، فالإنسان كما يقول أحد أدعيائهم- مخلوق له هذا القدر من حرية التصرف، الذي يمكنه - في أي مرحلة من مراحل تطوره - أن يضع آلهته كما يحلو له، فالحضارة التي صنعت الأقمار الصناعية والمركبات الفضائية والعقول الإلكترونية ليست في حاجة إلى آلهة... ! لقد فاق عبدة التكنولوجيا هؤلاء، أن كل ما صنعوه من إيديولوجيات، فشل في حسم تناقضات عالمهم، وفي تلبية الحد الأدنى من مطالبة الاجتماعية والنفسية.

لقد اثبت أهل الإنتروبولوجيا وعلم الاجتماع ما للدين من أهمية في منظومة المجتمع، فهو أي الدين ليس مجرد ظاهرة نفسية كما أكد لنا دور قايم بل هو أحد الثوابت الاجتماعية التي لم تضمحل مع التقدم العلمي.

تأتينا تكنولوجيا المعلومات وعولمتها، لتنذرنا بعالم جديد مليء بالاحتمالات وعدم اليقين، وكأننا مساقون إلى مصير لا ندري عنه شيئاً، فنحن نعيش عالماً تاهت فيه - من فرط تعقده- المعالم الفاصلة بين النظام والفوضى، وبين الخاص والعام، وبين الذاتي والموضوعي، وبين الحياة في عالم الواقع، وسكنى الفضاء الرمزي.

مع هذا وذاك جاءتنا تكنولوجيا المعلومات بحضارة جديدة، تكاد تكون مختلفة جملة وتفصيلاً عن الحضارات السابقة، ويمكن أن نطلق عليها تسمية (حضارة تكنولوجيا المعلومات)، وهذا النوع من الحضارة الجديدة على الإنسانية، والتي حطمت الحواجز والحدود ليس بين الدول فحسب، وإنما ما بين العلوم وجوانب الخير والشر، حيث بات المجتمع يعيش في متاهة الألف باب، لقد ارتكبت حضارة العصر تلك الخطايا التي حذرنا منها المهاتما غاندي: سياسة بلا مبادىء، وتجارة بلا أخلاق، وثروة بلا عمل، وتعليم بلا تربية، وعلم بلا ضمير، وعبادة بلا تضحية، وها

نحن في الألفية الثالثة، وخمس بالغينا من الأميّن ونصف صغارنا محرومون من المدارس، وأربعة أخماس عمالتنا مهددة بالبطالة، ولم تعد تنطلي على أحد تلك الوعود المسرفة، والتي لا هدف من ورائها، إلا أن يتحمل البؤساء والضعفاء مزيداً من البؤس والقهر انتظاراً لغد ذهبي قادم لا محالة، ما إن تتحقق الفروض، وتستتب الأمور تحت سلطة قوانين السوق. ولم يعد مقبولاً أن تقوم رأسمالية عصرنا بدلالة أرقام حساباتها دون غيرها كما وأطب على القول ماكس فيبر، ولم يعد هنالك من هو مستعد لدفع الكلفة الباهظة الناجمة عن المخاطر المتعددة من جراء التطبيق الأعمى لتكنولوجيا جسوره مجازفة غير مأمونة العواقب(١٩).

هكذا يبدو لنا جزء يسير من مخاطر تكنولوجيا المعلومات التي بات ينظر إليها الجميع بعين ملؤها الريبة إلى ما تدعيه هذه التكنولوجيا من نجاح. لقد صرنا نرهب النجاح بقدر ما نخشى الفشل، وتنامى لدينا الشعور بعجز عقولنا عن إنقاذنا مما صنعته أيدينا، لا نستطيع فكاكا من قبضة التكنولوجيا، التي توهمنا أنها تحت سيطرتنا، وقد انطلقت من قمقمها تدفع بنا نحو مصير مجهول، إنها تكنولوجيا مصابة بداء الحصاد- كما وصفها هيدجر- حصاد الطبيعة وحصاد الأجساد وحصاد العقول. لقد حق لنا - إزاء كل هذا- أن نسأل ونتساءل: هل ينذر عصر المعلومات بطوبائية رأسمالية سوداء؟ أم يبشر بعالم يعاد بناؤه من جديد، على أسس أخلاقية مغايرة، ترفض الوضعية العلمية وضلعها الفكري؟ وترفض البراجماتية ونفعيتها القصيرة النظر، وترفض ذاتية ما بعد الحداثة وقد اقتربت في رأي البعض- من حد الفوضى التي يمكن أن تؤدي بنا وبحضارتنا إلى موارد الهلاك، وبصورة أكثر تحديداً، هل يمكن لتكنولوجيا المعلومات أن تحقق نوعاً من الوئام بين ثلاثة الهداية والنظرة الشاملة والعقل؟ ثلاثية (الدين والفلسفة والعلم) كي نقيم على أساسها واقعية أكثر توازناً، تبحث عن الحق دون تضحي بالخير، وتتمسك بالخير دون إغفال الجمال.(٢٠)

أحدثت تكنولوجيا المعلومات ثورة في التواصل العلمي والمعرفي بين أبناء المعمورة، أينما كانوا، وفي أي زمان عاشوا من زمن عصر تكنولوجيا المعلومات، إنها ثورة تختلف عن الكثير من الثورات التي سبقتها، من حيث طبيعتها وأهدافها، ووظيفتها، فإذا كانت الثورات التي سبقتها من حيث طبيعتها وأهدافها ووظيفتها، فإذا كانت الثورات السياسية تحدث تغيراً ملحوظاً في الجوانب السياسية والاقتصادية، فإن ثورة تكنولوجيا المعلومات أحدثت بركاناً من التغيير، ليس في الجانب السياسي والاقتصادي فحسب، إنما في كل مجالات الحياة الاجتماعية منها والثقافية والعلمية والعسكرية.... الخ.

تعدد في مجتمع اليوم وسائل الحصول على المعلومة على نحو لم يكن متاحاً من قبل، وينطبق هذا على كل الجوانب التي يشغل المرء نفسه في الحياة، وكل الأسئلة التي تجول في خلده، وتتطلب الإجابة عنها. ومعظم هذه الوسائل قد صار تقليدياً، كالصحف والمجلات، والدوريات، والنشرات الخاصة، المحلية والدولية، فضلاً عن الإذاعات التي تغطي العالم بأسره، والقنوات التلفازية المختلفة، الإخبارية وغير الإخبارية، وهذه الوسائل المتنوعة قد ربطت بينها وسيلة أحدث هي شبكة المعلومات العالمية ، الإنترنت (internet). إن الثورة التكنولوجية بصفة عامة، وثورة الإنترنت بشكل خاص، تفرض نفسها فرضاً، وتطور نفسها يوماً بعد يوم، على نحو يثير الأسئلة حول الغايات العملية المنوطة بها، وإلى أي مدى هي واعدة برفاهية الإنسان، وما إذا كانت تنطوي في الوقت نفسه على تهديد مباشر أو غير مباشر لقيم الجماعة البشرية.

لعل أكثر وأكبر مخاطر تكنولوجيا المعلومات تكمن في شبكة المعلومات العالمية: الإنترنت، إن لشبكة المعلومات ميزة عظيمة في بعض الأحوال، وخطراً بالغاً في أحوال أخرى، أما الميزة فتتمثل في أنها مدخل حر إلى المعلومة، متاح للجميع، ومتاح كذلك في المناطق التي لا تمارس فيها العدية على نطاق واسع عن غير هذا الطريق، وأما الجانب السلبي لشبكة المعلومات فيتمثل في أنها غير خاضعة للمراقبة والتحكم؛ فليس هناك مؤسسة تقوم بالإشراف عليها، والواقع أنه من غير الممكن أن توضع الشبكة تحت الرقابة، وفي هذا يتمثل الخطر العظيم لسوء الاستعمال. إننا نسمع مراراً وتكراراً عن المضمون الإباحي والشعارات السياسية المتطرفة، والسباب الذي يتعرض له الساسة على شبكة المعلومات. وفي بعض الأحيان نجد الإشاعات التي يراد بها الإساءة أو التشكيل قد بدأت من الشبكة، من الموقع الغفل الآمن، وأدت إلى انتشار حكايات إخبارية لا أساس لها من الصحة. وهذا هو ثمن الحرية غير المنضبطة.(٢١).

تأتي المخاوف من الحرية غير المنظمة من واقع فعلي وملموس، ولعل الأسئلة الأهم التي تتجسد فيها الأخطار والمخاوف، مفادها: من الذي يملك الإنترنت؟ ومن الذي يديرها؟ أسئلة مشروعة روادت مخيلة العديد من المستخدمين للشبكة والدارسين لآثارها ومدى الخدمات التي تؤديها للبشرية، ولأن الناس اعتادوا دائماً على أن تكون الأشياء مملوكة من قبل أفراد أو مؤسسات وجهات أهلية كانت حكومية، مثل التلفونات... الكهرباء... والنقل، والطيران، وما شاكلها من الخدمات المركزية التي يتعامل معها الإنسان في كل يوم، فهم يتساءلون عن المالك الجديد لهذه الخدمة الجديدة ويضربون لذلك بالتلفون، فبالرغم من أن صاحب المنزل أو المكتب أو المؤسسة يوفر معدات الاستقبال في منزله أو مكتبه، ويقصد به جهاز التلفون (telephone set)، فإن

الربط بين المنزل والشركة المركزية للتلفون يتم عبر توصيلات تملكها الشركة، والمقسم الذي يستقبل المحادثات ويوجهها إلى الجهات التي يريد المشترك الاتصال بها تملكه الشركة أيضاً، والمستفيد من الخدمة يدفع مقابل استخدام هذه الشبكة أجراً للشركة، ولكنه في حالة الاتصال الداخلي كالاتصال التلفوني بين المكاتب في الوزارة مثلاً بواسطة تلفونات داخلية (intercom system)، فإن الشركة لا تتقاضى عليه أجراً، ولكن بمجرد الخروج من دائرة الوزارة أو الجامعة أو الشركة للاتصال بجهات أخرى فهي التي تقوم بالتوصيل بالأطراف الخارجية وهي التي تقدم التسهيلات من خلال شبكتها السلكية والمقسم للربط بين المشترك ومن يريد الاتصال به.

إذا طبقنا هذا التصور على شبكة الإنترنت نجد أن هناك تشابهاً في الجزء الخاص بتوفير معدات الاتصال من قبل المستفيد من الخدمة، وفي هذه الحالة الحاسب الآلي والمودم ولكي يتم الاتصال بالشبكة فلا بد من استخدام شبكة الجهة المسؤولة عن الاتصالات.

وعندما يتم الاتصال بالجهة المستهدفة وهي شبكة الإنترنت فلا نجد أحداً يطالب بحقه باعتبار أنه المالك المركزي للشبكة، إذ لا أحد يملك الإنترنت، وهذا يمثل مكامن الخطر الذي تلعبه شبكة الإنترنت.

فصاحب الكمبيوتر الذي دخل الشبكة يملك الكمبيوتر وبنفس القدر يملك شريحة في الشبكة تعادل الكمبيوتر الذي يستخدمه، وشركة الاتصالات تملك جزءاً من الشبكة وهو الجزء الموصل بين صاحب الحاسب الآلي والشبكة، وكلاهما جزء من الشبكة الدولية للإنترنت وإحدى عناصرها المكملة لها. والإنترنت لا يملكها أحد، ولا يسيطر عليها أحد،إنها ملكية تعاونية للجميع كل بقدر إسهامه فيها.(٢٢)

إن عدم امتلاك الإنترنت من قبل جهة مركزية ومحددة من جهة، وعدم وجود جهة تسيطر عليها من جهة أخرى، يمثلان أكبر مخاطر تكنولوجيا المعلومات، ومثل هذه الأمور دعت العديد من الناس أن يتصرفوا وفي ذهنهم عدم وجود رقيب وحسيب يعقب وراء تصرفاتهم، وبالتالي أدت تلك التصرفات إلى ما يسمى بالحرية غير المنضبطة.

بيد أن أمر خطورة تكنولوجيا المعلومات لا يتوقف عند هذه النقطة، إنما تجسد في نقطة أخرى ربما هي التي دعت الناس إلى التصرف اللامسؤول أو الخارج عن حدود المعقول، وهذا الخطر يتجسد في السؤال من الذي يدير الإنترنت؟ إنه بلا شك سؤال منطقي ولا يقل من حيث

أهميته وخطورته من السؤال السابق وهو إذا لم تكن الإنترنت مملوكة لأحد، وليس هناك سلطة مركزية تتولى أمرها، فمن الذي يديرها إذن؟ والإجابة عن هذا السؤال قد تفاجأ الكثيرون عندما يتضح لهم عدم وجود إدارة مركزية للإنترنت، لقد وصفها البعض بأنها فوضى تعاونية (cooperative anarchy)، فكل شبكة مشتركة في الإنترنت لها قواعدها الخاصة وهيكلها التنظيمي لإدارتها ولكن الإتصال بين الشبكات لا يمكن أن يحدث إلا إذا كان هناك تعاون بينهما، ولهذا فإن هناك عدداً من اللجان ومجموعات عمل تمثل فيها كل شركات المعلومات، وهي في اجتماعات مستمرة للوصول إلى وضع الأسس والضمانات التي تكفل تحسين الأداء في الشبكة وتطوير أسلوب التشغيل والاتفاق على المصطلحات والمستجدات التكنولوجية التي قد تطرأ بين حين وآخر.

يتضح مما سبق أن الإنترنت لا يملكها أحد، بل يملكها الجميع كل بقدر إسهامه فيها، ومقدار المعلومات التي يدخلها في الشبكة من خلال حاسبه الآلي أو شبكته المكونة من عدد من الحاسبات الآلية، ولا تديرها جهة مركزية معينة، بل الكل يشترك في إدارتها ويضعون القواعد والنظم التي يرتضونها جميعاً، وكل شبكة تشترك في الإنترنت تدير نفسها بالطريقة التي يراها أعضاؤها أو مجتمعها وليس هناك قانون تفرضه عليها الإنترنت، وهذه المعلومات والمبادئ هي التي تسير الإنترنت، وهي التي تحكم حركتها واتجاهها، والإحاطة بكل هذه المعلومات أمر ضروري لكل من يريد أن يدخل في الشبكة ويستفيد بما فيها من كنوز المعرفة ومحيطات من المعلومات بأشكالها وأنواعها المختلفة(٢٣).

وفق المعطيات السابقة يتضح أن الهامش الواسع من الحرية ربما هو الذي يقود العديد من الناس الذين بطابعهم الإساءة أن يرتكبوا أعمالاً إجرامية بحق الآخرين، ولكن عن بعد، وهذا يعد الخطر الأكبر الذي يهدد حياة وأمن وأمان المجتمعات، وهذا ما سمحت به، ومن خلالها تكنولوجيا المعلومات لكونها أصبحت أداة طبيعية بيد مثل هذه النفوس الشريرة.

تتضح بشكل لافت للنظر مخاطر تكنولوجيا المعلومات وتحديداً تكنولوجيا الاتصال منها، بوصفها أداة إعلامية عند عمل مقارنة بينها (تكنولوجيا الاتصالات) وبين وسائل الإعلام الأخرى. في واقع الأمر إن وسائل الإعلام كانت دائماً إذا نظرنا إلى وظيفتها الصحيحة تقوم على خدمة المجتمع لا على المستوى الفردي، ولكن على المستوى الجماعي، بمعنى أنها تأخذ في الحسبان الخاصية للمجتمع بما ينطوي عليه هذا من قيم وأعراف وعلاقات مشتركة تميّز هذا المجتمع. ومن

هنا عرفت وسائل الإعلام التقليدية على اختلافها أسلوب الرقابة، سواء مورست هذه الرقابة من أجهـزة خارجهـا أو تأصلت في نظام العمل داخلها. وبغض النظر الآن عما قد يكـون في بعـض الأحيـان مـن إسـاءة اسـتخدام هـذا الأسـلوب عندما تمارسه أجهزة رقابية خارجية، تظل هذه الممارسة في شكلها مستهدفة دعم البنية الكلية للجماعة والمحافظـة عـلى ترابطها وتماسكها ووقوف أفرادها على حد من الأرض المشتركة، هذه الصورة، أو هذه الوضعية، تتراجع الآن شـيئاً فـشيئاً أمام الانتشار السريع، بل الكاسح لشبكة المعلومات واتساع نطاق المتعاملين معها(٢٤).

تظهر بجلاء مخاطر تكنولوجيا المعلومات من انتهاء وتفريغ العديد من القوانين الرقابية مـن محتواهـا التـي ترصـد تدفق المعلومات عبر الحدود الجغرافية القومية، لقد أصبح العديد من قوانين الرقابة على تدفق المعلومات عبر الحـدود القومية مجرد نصوص فارغة لا معنى لها، ولا تأثير حقيقي لوجودها ، بل أصبح مبرر احتكار الدولة لسلطة تنظـيم بيئـة الاتصال والمعلومات أمراً ينتمي للماضي البعيد، فقد كانت الدولة تتـدخل في حقـل الإعـلام لمنـع الاحتكـار، ولا تـستخدم الإعلام في أدوار اجتماعية، اعتماداً على ندوة المجال طبيعة موجات البث وقنوات التوصيل التي تبدو نهائية)، أمـا اليـوم فإن تفجر منافـذ وسـائل الأعـلام وأدوات التوصـيل، وتكنولوجيـا اتـصالات الأليـاف البـصرية التـي يمكنهـا حمـل ملايـين المعلومات والصور الرقمية- قضى على شرعية فكرة التنظيـم العـام، وهكـذا سـقط مـبرر احتكـار الدولـة لقيـادة النظـام الإعلامي وتنظيمه ، كما تراجع دورها الفاعل في النظام الإعلامي نتيجة الثورة التي أحدثتها تكنولوجيا الاتصال.(٢٥)

تأتي المخاوف والمخاطر من تكنولوجيا الاتصال وتحديداً من شبكة الإنترنت لسبب وجيه، ويكمـن في العـالم الرحـب والواسع الذي تغطيه هذه الشبكة، لقد بات الناس وأصبحوا، وهم يصفون الإنترنـت بأنهـا فـسيحة رحبـة ومتغـيرة عـلى الدوام، ولا أحد يدّعي أنه سيدها ، ولم يستطع أحد أن يغوص في أعماقها ويسبر غورها، ولا أحـد يعـرف كـل شيء عنهـا؛ لأنها تتغير كل يوم. ولكنك كالربان الماهر تستطيع أن ترسم خريطة للبحار التي اعتدت السفر عليها وتتعلم أيضاً كيـف تسافر بسلامة على تلك التي لم تجرب السفر عليها وتتعلم أيضاً كيف تسافر بـسلامة عـلى تلـك التـي لم تجـرب الـسفر عليها من قبل، فتعود من رحلتك الجديدة وأنت تحمل من كل رحلة فيما بعد بالكنوز والمعلومات الجديدة.(٢٦)

وفق ذلك يبقى هذا الربان (المستفيد) هو ذلك الذي يملك زمام الأمور، إذ بإمكانه أن يقود السفينة إلى بـر الأمـان، وفي ذات الآن، بإمكانه أن يقود ذات السفينة على حالة الخطر والغرق،

وعندها لا يغرق ربان السفينة وحده، بل يُغرق الآخرين معه (بعض أفراد المجتمع)، وهذا يمثل أهم مخاطر تكنولوجيا المعلومات، عندما لا يستطيع المستفيد كبح جماح نفسه، والتي تقوده إلى ارتكاب جرائم بحق نفسه أولاً وبحق الآخرين ثانياً، وحالة عدم كبح الجماح متأتية من عدم وجود الرقيب المتعارف عليه في الوسائط الأخرى.

لقد صار من السهل على كل من امتلك خطاً تليفونيا وحاسوباً شخصياً، أن يدخل إلى الشبكة، وربما من هنا تبدأ أولى الخطوات نحو مكامن خطر تكنولوجيا المعلومات، على اعتبار أن هذا الشخص المتصل بعيداً عن عيون الرقيب والرقابة. والخطوة الثانية نحو مكامن الخطر لها علاقة بالخطوة الأولى، إذ يكاد يكون من المحال استخدام الرقابة في حذف ما هو سيء أو غير مرغوب فيه، على نحو ما كانت نظم الحكم الشمولي تصنع مع الصحف. ولا سبيل في الواقع لإسكات هذه الوسيلة الإعلامية إلا بالاستيلاء على أجهزة كمبيوتر المواطنين الشخصية، وعلى خطوط تليفوناتهم، وهو اختيار يندر قبوله اليوم في كثير من البلدان.

حقاً إن وسائل الإعلام الجماهيرية التقليدية قد لا تكون مثالية في عملها، ولكنها تؤدي هذا العمل في حدود معايير معروفة ومصطلح عليها في أساسيات المهنة؛ فالتقارير والتحقيقات تمر من خلال عملية تحرير من شأنها أن تدققها قدر المستطاع، فإذا وقعت مع ذلك أخطاء فإنه يتم تداركها، وإذا لحقت الإساءة بأي طرف- شخصاً كان أو جماعة أو مؤسسة أو دولة.... الخ- وشعر بتشويه سمعته فإنه يستطيع أن يقاضي الوسيلة الإعلامية التي أساءت غليه. وهذا مالا يتحقق في حال استخدام الشبكة، فلا مراجعة ولا مؤاخذة. كذلك فإنك لا تعرف على وجه الدقة ما إذا كان الموقع على الشبكة يقدم إليك معلومة صحيحة أم لا عن موضوع ما. وربما كان أسوأ من هذا أن يدعي أصحاب موقع من المواقع على الشبكة، أنه يقوم ببث أخبار غير منحازة إلى طرف ما، وهم يعلمون أنهم ينشرون الشائعات التي تفضي إلى المقاضاة لو أنها ظهرت في وسائل الأعلام المألوفة. ومع ذلك فإنه على الرغم من هذه الأخطار وما شابهها مما قد ينجم عن استخدام شبكة المعلومات، لا يملك أحد أن يوقف انتشارها الكاسح، حتى لقد أوشكت أن تصبح جزءاً لا يتجزأ من الحياة.

بيد أن السؤال الذي يظل يشغل فكر الكثير من الناس مفاده: ماذا عن أثر هذه الشبكة في الواقع البشري في حياة الفرد والجماعة على السواء؟ أو لنقل ما التغيير الذي ينتظر أن تحدثه في حياتهم؟ يذهب (دافيد هيوسن إلى أن) (الشبكة في الحقيقة لا تغير الناس ، ولكن الناس هم

الذين يغيرون الشبكة) وربما كانت الصيغة الأدق للحقيقة في هذا الصدد هي أن الناس إذ يغيرون الشبكة يتغيرون هم أنفسهم كذلك، بمعنى أنهم بقدر ما يغيرون الشبكة تغيرهم الشبكة كذلك بالضرورة.

فعلى سبيل المثال، فإنه بقدر ما يكون امتداد الشبكة بحيث تغطي أكبر قدر من الأخبار العالمية يكون انهماك الأفراد في الجلوس إلى الجهاز لقراءة هذه الأخبار على شاشته، أو حتى رؤية الأحداث مصورة في مواقعها، والاستغناء بهذا عن قراءة الصحف وعن شرائها واقتنائها وفي هذا السياق شبه الدكتور (فين سيرف) المشهور بأنه أبو الشبكة العالمية - شبه تأثير الإنترنت في مسيرة البشرية الآن بالتأثير الذي أحدثه ظهور المحركات والكهرباء وتغلغلها في مسيرة حياة الناس حتى أصبحت المحركات تعمل على مدار اليوم والأسبوع والسنة بلا توقف، ومن شدة انتشارها تحولت إلى شيء شائع وجزء لا يتجزأ من الحياة، لا يشعر أحد بوجوده إلى حينما يتعطل عن العمل. وهكذا بدأت الإنترنت وتكنولوجيا المعلومات عموماً تلعب دوراً مشابهاً، يتحول بسرعة على جزء من نسج الحياة العامة لكل الناس، يتعايشون معه ويألفونه، ويذوب في تفاصيل حياتهم اليومية.

تظهر بجلاء بؤرة خطر تكنولوجيا المعلومات في شبكة المعلومات العالمية، حيث إن الشبكة العالمية (worldwide web) تقوم على أساس من تكنولوجيا (الجذب) (Pull Technology)، وهذا يعني أن مستخدم الشبكة ينبغي له أن يطلب صفحة من صفحاتها قبل أن ترسل إليه. وعلى النقيض، تقوم الإذاعة على أساس تكنولوجيا الدفع (Push Technology)، وذلك لأنها ترسل المعلومات بغض النظر عما إذا كان هناك من يستقبلها.(٢٧)

تنجلي بوضوح خطورة تكنولوجيا المعلومات في جانب مهم وخطير جداً في ذات الآن، ألا وهو "حرية التعبير والرقابة"، إذ أن أحد أشكال التعبير التي ينفرد بها الاتصال المباشر عبر أجهزة الكمبيوتر (online communication) هي أن يُعبّر الإنسان عن غيظه بأن يقوم بكتابة رسالة مباشرة عبر جهاز الكمبيوتر. وقد تحوي هذه الرسالة ازدراءً، وأقوالاً فاحشة أو لغة غير مناسبة. وللأسف، فإن القوانين التي تحمي الفرد عندما يتحدث في التيلفون أو يستمع إلى الراديو أو يشاهد التلفاز- لا تستطيع أن تحميه من البذاءات التي قد يحملها البريد الالكتروني إلى عقر داره. إن البذاءات التي ترد عبر البريد الإلكتروني، لا يمكن أن تُقال في التليفون، ولا يمكن أن يتفوه بها شخص في وجه آخر. وقد تأتي هذه الألفاظ، المشينة في خطاب، ولكن بعض الأشخاص سوف

يفكرون مرتين قبل إرسال مثل هذا الخطاب، ولكن البريد الإلكتروني يفتح الباب واسعاً لأن يرسلوا أيـة رسـائل طالمـا لا يوجد دليل لإدانة ما قد تحمله هذه الرسائل من أشياء يعاقب عليها القانون.(٢٨).

ربما هذا يعد أخطر ما يمكن أن تفعله تكنولوجيا المعلومات على الأفراد والمجتمع وما تتركه من آثار ومخاطر سلبية في بنية أخلاق المجتمع. فقد فتحت الطرق على مصراعيها للناس، فباتت حرية التعبير غير المنضبطة يمارسها العديـد مـن الناس الذين لا يُقدّرون معنـى الحريـة، وبـاتوا يـستخدمون تكنولوجيـا المعلومـات لأغـراض خارجـة عـن حـدود الأدب والأخلاق المتعارف عليها. وبدأت عملية الإساءة إلى العديد من الناس المحترمين ممكنة في ظل غيـاب الرقيـب أو القـانون الذي يردع مثل هؤلاء، ومثل هذه العمليات جعلت من تكنولوجيا المعلومات أداة للتجاوز على حدود وحقوق الآخـرين في ظل غياب القانون في مثل هذه الحالات.

إن طبيعة البريد الإلكتروني تتمثل في أن الفرد لا يفكر مرتين قبل أن يكتب رسالته، فهو يكتب ويرسل ما يكتبه عـلى الفور. كما أنه في البريد الإلكتروني لا تتضح الصفات الحاسمة لشخصية الفرد، التي يمكن أن تـتـضح في الحـال في الاتـصال المواجهي (القائم على المواجهـة وجهـاً لوجـه) (Face-to-face communication) وهـو مـالا يمكـن إفـشاؤه في الاتـصالات المباشرة عبر الكمبيوتر، وعلاوة على ذلك، فإن كثيراً من الأفراد يستخدمون ألقاباً بدلاً مـن اسـتخدام أسـمائهم الحقيقيـة عند اللجوء إلى البريد الالكتروني (٢٩).

تزداد مخاوف الناس أكثر، ويزداد خطر تكنولوجيا المعلومات أكثر وأعمق، عندما يتعلق الأمـر بالأطفـال، لا سـيما في مرحلة المراهقة، يتضح الخطر هنا عندما يتعلق الأمر بالإنترنت، وكما يحلو للـبعض أن يلقـبهم بـشاب وصـبايا الإنترنـت (لمجرد التعبير عن وثاقة الصلة بين مرحلة المراهقة وبين الاستخدام المكثف للإنترنت) فإن وضعهم يختلف كثيراً لإختلاف سمات هذه المرحلة، فهذه المرحلة العمرية الانتقالية في حياة الإنسان، مرحلة إثبات الذات والإسـتقلالية، والتميـز وبنـاء الشخصية والحرية (كما يرددون) (وهنا يكمـن خطـر العلاقـة بـين الأطفـال وتكنولوجيـا المعلومـات) وفي هـذه المرحلـة العمرية بالذات ينتشر استخدام الإنترنت لعدة أغراض واهتمامات يمكن من خلالها التنبؤ بشخصية المراهق وحيث تـأتي التطبيقات الأتية ضمن أولويات استخدام الإنترنت:

١- الدردشة أو الحوار (Chatting) بكافة أشكاله، المكتوب والمسموع والمرئي.

٢- تبادل رسائل البريد الالكتروني E-MALL مع الأصدقاء.

٣- إرسال رسائل قصيرة للهواتف المحمولة (Mobile massages) التي يمتلكها الأصدقاء والأقرباء.

٤- الاستماع إلى الموسيقى ومشاهدة الأغاني المصورة ومقتطفات الأفلام السينمائية.

٥- المشاركة في الألعاب الإلكترونية الشيقة الجذابة المتاحة على الإنترنت.

٦- تصفح الصحف والمجلات وغيرها من مصادر المعلومات المتجددة والتي يمكن أن تقدم معلومات عن الأحداث الجارية المحلية والعالمية وخصوصاً في مجالات الرياضة والسياسة والأزياء... الخ.

قبل دخول الإنترنت، لم تقلقنا تلك الاستخدامات؛ لأن معظمها مألوفاً لدينا، مثل تبادل الرسائل والاستماع إلى الموسيقى ومشاهدة الأفلام، والألعاب الإلكترونية وقراءة الصحف والمجلات، كما أن إرسال الرسائل القصيرة للهواتف المحمولة خدمة تقدمها شبكات تلك الهواتف دون الحاجة إلى استخدام الإنترنت، ولكن ما تتميز به هذه العملية حينما تتم عن طريق الإنترنت هو بقاء المرسل مجهولاً لدى المستقبل مما يعني التعبير الحرفي كتابة تلك الرسائل (ولا داعي أن أوضح إلى أي مدى يمكن أن تصل تلك الحرية في التعبير عند كثير من المراهقين. (٣٠)

لعل أعلى درجات الخطر تكمن في العلاقة بين الأطفال والشباب والإنترنت عندما يصبح هؤلاء قد وصلوا مرحلة الإدمان أو يطلق عليها أحياناً (مدمنوا الحوار عبر الانترنت) يعتقد البعض أنه لا يوجد مراهق من الجنسين لم يدمن الحوار أو الدردشة (chatting) من خلال مئات المواقع المتاحة على الإنترنت سواء باللغة العربية أو باي لغة أجنبية أخرى يجيدها المراهق والتي غالباً ما تكون الإنجليزية إن تلك المواقع المخصصة للدردشة أو الحوار قد تم تجهيزها بالعديد من غرف الحوار تجهيزاً مسبقاً، كما أنها تترك للمستخدم حرية تجهيز غرف أخرى لم يسبق التجهيز لها، وفي حالة احترام الحوار بين طرفيه وارتفاع درجة حرارة الدردشة، وحرصاً من إدارة الموقع على عدم تأثر المتحاورين الآخرين بتلك الحرارة، فإنه بالإمكان الانفصال والإبتعاد عن غرفة الحوار الجماعي والاستقلال في غرفة خاصة لا يسمح بدخولها أحد غير هذين المتحابين (أعني المتحاورين). وتتبارى الهيئات المسؤولة عن تلك المواقع فيما بينها في تصنيف غرف الحوار وإطلاق تسميات جذابة

عليها، هذا بخلاف أنها تترك الحرية أمام المتحاورين لإطلاق ما يحلو لهم من تسميات يمكن أن تعبر تعبيراً حراً عـن طبيعة موضوعات الحوار.

تأتي المخاوف من العلاقة بين الأطفال والإنترنت من جانب آخر يتعلق هـذه المـرة في الجانـب الاجتماعـي والنفـسي لجدوى الحوار مع أشخاص مجهولين تماماً قد يبدو ذكوراً وهم في الواقع إناث أو العكس، وقد يبدو كباراً وهم في الواقع أطفالاً، وهكذا لا يعلم بحقيقتهم وبواقعهم إلا اللـه سبحانه وتعالى. فكيف إذا تتكون الصداقة وتنمو في ظل مناخ مـن عدم الثقة؟ فإذا كنا نحن في الحياة الواقعية لا نقبل على مصادقة إنسان قبل أن تثبت لنا مواقفه وأفعاله جدراته بذلك، فكيف يتحقق ذلك من خلال شاشة الكمبيوتر(٣١)؟؟؟

بيد أن الأمر كثيراً ما يستدعي المهتمين بشؤون تربية الأطفال وتنشئتهم إلى طرح عـدة تـساؤلات مهمـة منهـا: هـل انشغال أولياء الأمور عن أبنائهم هـو الـدافع وراء اللجـوء إلى الحـوار المجهـول؟ أم أن ضـعف شخـصية المراهـق وعـدم مقدرته على الحوار المباشر وراء هسترية الحوار عبر الإنترنت؟ وهـل الرغبـة في التعـرف إلى الجـنس الآخـر دون ارتكـاب ذنب أو معصية اللقاء المباشر، وفي بعض الأحيان صعوبة هذا اللقاء، مثيراً وسبباً وحـافزاً لهـذه الحـوارات؟ أم أن اختفـاء الهوية (هوية كل من المرسل والمستقبل) بكل ما تحمله من سمات (الاسم ، الشكل، الطباع، المستوى التعليمـي، الحالـة الاجتماعية، الحالة الاقتصادية،...الخ) دافعاً قوياً للاعتقاد والتـوهم بأنـه لا توجـد فـوارق أو طبقـات اجتماعيـة وبالتـالي انطلق وتحدث وتحاور مع من تشاء وارتبط عاطفياً بمن تحب؟ وهكذا تسير الأمور غير الفضاء المعلوماتي.

تتجسد المخاوف أكثر فأكثر ، عندما تقدم الإنترنت وجبة دسمة من الجنس أصابت المجتمعات بقرحة شديدة في الأمعاء، وسببت في الآن ذاته صداع ليس فقط للمعنيين والمهتمين بشؤون وتربية الأطفال، بل أقلقت الحكومات ذاتها، إذا لم تتوقع الحكومات هذا الكم الهائل من المواد الجنسية على اختلاف أشكال إتاحتها (المباشر أو الحي غير المباشر أو المسجل)

(الصورة الثابتة والفيديو) (الحوار والمشاهدة) (الجنس الطبيعي والشاذ) (المراهقون والكبار)... الخ.. من الاختيارات والرغبات والأهداف التي تتعلق بعرق أو بلدة معينة أو بلون بشرة أو حتى بحجم جسدي معين.. وهكذا تتنوع الاختيارات أمام المستخدم لدرجة تشعره بأن الانترنت قد وجدت في الأصل لخدمة مثل هذه الأغراض، ويعتقد أنه لولا هذه الجرعات المكثفة من المواد الجنسية لما ذاع

صيت الإنترنت وانتشرت بهذه السرعة؟؟؟!! أو التوهم بأن الإنترنت بالإضافة لكونها شبكة عالمية للمعلومات فهي عولمة لشبكات الدعارة المحلية.(٣٢).

هكذا تتولد المخاوف والمخاطر يوماً بعد يوم، ويظهر المكنون من مخاطر تكنولوجيا المعلومات، بيد أن اللافت للنظر في هذا الأمر، يتمثل في أن المواد والمواقع الإباحية لم تقف عند حدود دولة معينة، أو تتحملها جبهة أو منظمة أو دولة بعينها، بل يبدو أن الأمر يشير إلى مشاركة دولة عربية وإسلامية، ولها مواقع على الإنترنت، وهذا يمثل الخطر بعينه، فعندما تُهاجم من الخارج معنى ذلك أنك حددت هوية عدوك، إلا أن الأمر يختلف عندما تُهاجم من الداخل فلا تستطيع أن تحدد هوية عدوك على اعتبار أن من في الداخل على الأعم الأغلب هو أخيك؟؟ وهذا الداء الذي يصعب أن تصف له الدواء في ظل جرائم تكنولوجيا المعلومات.

٤- جحيم تكنولوجيا المعلومات المرفوض.

تمثل الإنترنت قمة ما توصلت إليه تكنولوجيا المعلومات، وهي بذلك تمثل قمة التحدي للإنسانية في ذات الوقت، إذ أنها – أي الإنترنت لم تعد الرئة التي يتنفس من خلالها المجتمع، بل الشرايين التي توصل الدم بين أجزاء الجسم كافة، ولذلك لا يجوز الحديث دائماً عن الإيجابيات فقط، وننسى أو نتناسى السلبيات ولعل السؤال الأكيد الذي يبرز هنا بشكل لافت للنظر مفاده من أين يأتي الجانب السلبي لتكنولوجيا المعلومات؟ ولماذا خلقت تكنولوجيا المعلومات مناخاً أو جواً أقل ما يقال عنه بأنه جحيماً مرفوضاً؟

لقد جرى الحديث في صفحات سابقة عن تكنولوجيا المعلومات ومدى علاقتها بظاهرة العولمة وبالعكس إذ برز وبقوة في عالم اليوم ظاهرة جديدة آخذة في التبلور والتشكل بشكل سريع ومتواتر، وقد تغير من وجه الحضارة الإنسانية على نحو لم تشهده من قبل هذه الظاهرة أطلق عليها عدة مسميات : العولمة، الكونية، الكوكبة، ويمكن أن نستنتج من هذه التسميات الآثار السلبية والمخاطر التي تؤثر في المجتمع الإنساني، علماً أن مكونات العولمة الرئيسية هي:

١- توسع التجارة الدولية، ويقوم بهذا الدور (منظمة التجارة الدولية)، التي تسعى لفتح أسواق العالم أمام حركة الأموال، والاستثمارات والبضائع والخدمات وتكريس مبدأ التنافس والميزة التنافسية.

٢- الانفجار المعلوماتي، ويعني ذلك وفرة المعلومات وتراكمها بشكل سريع وإتاحتها للاستعمال عبر أوعية المعلومات وأهمها الحاسبات الآلية.

٣- ثورة الاتصالات، ويشهد هذا الجانب تطوراً تقنياً مذهلاً يسهل التواصل بن بني الإنسان عبرأ اتصالات مختلفة كالهاتف ، والفاكس، والأقمار الصناعية وأهمها جميعاً "الانترنت" فهي تؤدب الوظائف السابقة كلها، ويتنبأ المستقبليون أن هذه العناصر الثلاثة ستؤثر على جوانب حياة الإنسان الاجتماعية والاقتصادية والثقافية وستعمل على إيجاد هوية جديدة للإنسان هي: (الإنسان العالمي) وستخفي الهوية الوطنية أو القومية.

تسعى دول العالم منذ عقد اتفاقية (القات) في أورجواي- وقد بدأت قبل ذلك بكثير إلى زيادة التجارة الدولية وخفض التعرفة الجمركية للسماح للأموال والاستثمارات والسلع بالتنقل بحرية بين الدول، واندفع كثير من الدول النامية ودول شرق آسيا نحو هذا الإتجاه، وسمحت للأموال الأجنبية بالدخول إليها، ولم تكن هذه الأموال تستثمر في نواح تنموية حقيقية تعمل على توفير الهياكل الاقتصادية الحديثة أو تعمل على تطوير وتحديث الهياكل القائمة، أو رفع المستوى المعيشي والحضاري للإنسان وإنما كانت تهدف إلى الربح السريع عن طريق المضاربة في اسواق المال. وماذا حدث بعد سحب هذه الأموال؟ إنهارت اقتصاديات هذه الدول، وانهارت العملة، وحدثت اضطرابات اجتماعية وقادت إلى آثار أمنية مريعة، نهب وسرقة وتدمير... نشاهدها على شاشات التلفزة.

إن توفر المعلومات بشكل مكثف عن طريق الفضائيات التلفازية والإذاعية والصحف والمجلات... وغيرها، سمح بتمرير ونقل قيم ومفاهيم وأساليب معيشة وتفكير جديدة إلى مجتمعات العالم، وأصبحت للدول التي تملك الأدوات والوسائل المعلوماتية والإعلامية القدرة على فرض ثقافتها وقيمها، مما جعل بعض المجتمعات الغربية والشرقية على حد سواء تعمل على تحصين ثقافتها وخصوصيتها من التشويه.(٣٣) في حين ظلت الدول النامية التي لا تمتلك تكنولوجيا المعلومات متقدمة الأمن حيث صناعتها، ولا من حيث استيرادها، ظلت ثقافتها وخصوصيتها عادية ومعرضة للتعرية، وبالتالي فإن مثل هذه الدول غير قادرة على حماية ثقافتها وأمنها للوافد من الخارج.

يعيش الإنسان في مجتمع المعلومات اليوم، بين الفردوس المعلوماتي الموعود الذي يعد أنصاره العالم بأن الإنسانية ستتمتع في ضوئه بمجتمع للمعرفة غير مسبوق، وبين الجحيم المعلوماتي المرفوض الذي يبشر دعاته الإنسانية بمستقبل كئيب ومظلم، نظراً لهيمنة الكبار على المعلومات والمعرفة معاً، وبين الفردوس والجحيم يمكن أن تسقط الحقيقة! والذين يعدون الإنسانية بجحيم تكنولوجيا المعلومات لهم حججهم المنطقية في هذا المجال، إذ أن منطق هؤلاء المتشائمين يمكن

إجماله في عبارة جامعة هي: أنه مهما حسنت نياتهم، فإن هناك ثمن اقتصادي لا بد أن يدفع نتيجة تطبيق التكنولوجيات الجديدة، ولذلك فمن باب الخطأ أن نقفز من الفوائد الجزئية التي يمكن أن نجنيها منها، ونقدم صورة وردية عن آثارها، وكأن الجوانب السلبية والإيجابية سواء.(٣٤).

باتت تتمثل التحديات التي يستند عليها أصحاب الصورة المتشائمة التي واجهت المخططين والباحثين في تأثيرات الإنترنت هو ذلك التلازم بين انتشار تطبيقات الشبكة كوسيلة جماهيرية والآثار السلبية المتصاعدة والمحتملة لمختلف خدماتها، وتمثل الإنترنت حالة فريدة، حيث هي وسيلة اتصال لا يمكن تجاهلها، وهي أيضاً منتدى عالمي فيه أسواق وخدمات وغيرها تنشط التجارة العالمية، وهذه الأنشطة يرافقها بطبيعة الحال، ما يرافق الأنشطة التجاري عادة من غش واحتيال وعرض سلع ممنوعة ونحو ذلك، وهي أيضاً ملتقى للباحثين والعلماء، وأيضاً هي ناد عالمي مفتوح للمجرمين، والخارجين على القانون. وعند النظر إلى الانترنت من زاوية أمنية جنائية، فلا شك أن طبيعة الشبكة التفاعلية يمكن أن تسهم في تقديم خدمات كبرى للعصابات الإجرامية والمنظمات الإرهابية تمكنهم من خلالها من تبادل الاتصالات والمعلومات وإجراء المشاورات ووضع الخطط في غفلة عن عيون الأمن، وعلى الإنترنت أيضا تنتشر عشرات المواقع للجماعات العرقية والدينية المضطهدة وتستخدم بفعالية من قبل الكثير من الجماعات ذات التوجهات الفكرية والسياسية للاتصال والتنسيق بعد أن ضيقت عليها الأجهزة الرسمية قنوات الاتصال فيما بينها أو التواصل مع مؤيديها، وعلى سبيل المثال فقد ظهرت تقارير إعلامية تؤكد استخدام الإنترنت

وإمكاناتها الاتصالية للتنسيق من قبل منفذي الهجوم الكبير على برجي مركز التجارة العالمية في نيويورك ومبنى البنتاغون في الحادي عشر من سبتمر الماضي(٣٥).

إذا كان للمتفائلين حججهم التي يستندون عليها عندما يسرد من الجانب الإيجابي لتكنولوجيا المعلومات، فإن المتشائمين لهم ايضاً حججهم التي يستندون عليها، ويمكن تلخيص حجج المتشائمين في الشكل الآتي:

١- التعامل مع تكنولوجيا الاتصال والمعلومات الجديدة وكأنها بمثابة دين جديد، أو الإشارة إلى البشر باعتبارهم خالقين للتكنولوجيا قد يؤدي إلى ضياع القيم ومن ناحية أخرى الاعتراف بفضل التكنولوجيا الجديدة أو اعتبارها مسؤولة عن ممارستها قد يؤدي إلى إهمال البعد الإنساني، كما صرح البابا جون بول الثاني عام (١٩٩٨) حين قال: "إن التكنولوجيا الجديدة إله زائف"

٢- تنمو التكنولوجيا الجديدة بسرعة مذهلة، مما من شأنه أن يجعل المجتمعات الإنسانية لا تستطيع أن تتكيف معها لا هي ولا البشر، وأصبحت مهمة التنبؤ بالمستقبل بالغة الصعوبة. ومن المحتمل أن تكون أخطر المشكلات الناجمة عن الثورة المعلوماتية نفسية واجتماعية، ذلك أن فيض المعلومات على شبكة الإنترنت من شأنه أن يفقدها مصداقيتها وثباتها، ومن ناحية أخرى فإن هذا الفيض يعني ضيق الوقت أمام مستخدمي الشبكة لكي يحولوا هذه المعلومات إلى معرفة وتقييم وحكمة.

٣- هناك المخاطر المتمثلة في بزوغ إمبراطوريات جديدة للقوة، وشركات عملاقة، وكل ذلك مصحوب بخطر تصاعد الإقلال من إنسانية الحياة؛ وذلك إذا ما حلّت قيم السوق محل القيم الإنسانية الأخرى. وهيمنة القوة السياسية والاقتصادية قد تؤدي إلى ظهور مجتمعات شمولية. كما أن الثورة المعلوماتية قد تؤدي إلى ظهور قطاع الكتروني! ذلك أن تركز التكنولوجيا الجديدة في وحدات قليلة قد تؤدي إلى عدم المساواة والاستقطاب والاستبعاد.

٤- الهوّة بين الغنى المعلوماتي والفقر المعلوماتي قد تزداد، مصاحبة في ذلك عدم المساواة في الدخول. صحيح أن هذه الظواهر ليست جديدة لا على المستويات المحلية أو على المستوى الكوني، ولكن التكنولوجيات الجديدة قد تزيد الموقف سوءً. إن هذا من شأنه أن تنقرض الطبقة الوسطى، وتنمو إلى حد كبير طبقات المعدمين، الذين سيستبعدون من التقدم الإنساني ويصبحون معزولين ومهمشين.

٥- الثورة المعلوماتية تسهل نقل ونشر الثقافات المختلفة على مستوى العالم، غير أن هذه الإمكانية يمكن أن تؤدي على هيمنة ثقافية ولغوية في الفضاء المعرفي، كما أن نقل الثقافات وأساليب الحياة، وهي عملية غير مرّحب بها في المجتمعات، لاسيما المجتمعات المحافظة، ستصبح مسألة سهلة من خلال التكنولوجيا الجديدة، وعلى سبيل المثال، فإن أنماط الاستهلاك التي تعتبر أساسية بالنسبة لاقتصاديات الوفرة في المجتمعات الصناعية، يمكن أن تكون بالغة الضرر لاقتصاديات الدول النامية، وإذا ما مارست الشرائح الفنية في المجتمع هذه الأنماط الاستهلاكية، فإن ذلك قد يؤدي إلى مزيد من إفقاد باقي شرائح المجتمع.

٦- تهدد تكنولوجيا الاتصال والمعلومات الجديدة بخرق حقوق الخصوصية والحقوق المدنية الأساسية، ذلك أنها يمكن أن تستخدم عن طريق الأنشطة الإجرامية الفضائية سواء

بإرتكاب جرائم التزويد أو السرقة من خلال سهولة النفاذ إلى قواعد البيانات الشخصية، ويمكن أيضاً أن تستخدم لمراقبة معدلات الاداء في العمل، وسرقة الأموال، وكذلك سرقة البيانات، والدخول غير الشرعي على الشبكات، والاعتداء على سرية البيانات الشخصية، والتخريب العمري للشبكات، كل ذلك بالإضافة إلى نشر الصور الإباحية على الانترنت، مما يعرض الأطفال والشباب للخطر، بالإضافة إلى ممارسة الدعارة عن طريق الشبكة.

٧- تستفيد الميديا الفضائية والألعاب الإلكترونية من نقص التنظيم الذي يحكم حركتها وممارستها ومن الملكية الخاصة لها. وقد أصبح الأطفال أكثر تعرضاً للسيطرة عليهم من قبل هذه الشبكات الجديدة التي تقدم لها برامج متعددة مليئة بأحداث العنف، والتي تفتقر إلى أي مضمون حقيقي، أو إلى أي سياق اجتماعي، وقد أصبح واضحاً الآن بالنسبة للكبار والأطفال على السواء أن تمضية جزء كبير من وقتهم مع الواقع الافتراضي بدلاً من الواقع الحقيقي يمكن أن يؤدي إلى مزيد من عزلتهم الاجتماعية والشخصية.

٨- التكنولوجيا الجديدة تؤثر سلبياً على البيئة. ذلك أن انتاج الحاسبات الآلية يحتاج إلى استنزاف شديد للموارد.

٩- مع تسارع إيقاع ظهور المجتمعات المبنية على المعرفة، فإن الأفراد الذين هم بالفعل في وضع هامشي سواء في التعليم في الحياة الاجتماعية والاقتصادية سيجدون أنفسهم مستبعدين. وحتى بالنسبة للافراد ذوي المؤهلات المرتفعة فإن شعوراً بعدم الأمان ينتابهم. وبوجه عام يمكن القول: إن التكنولوجيا الجديدة ستؤثر سلباً على العمل، وستزداد البطالة.

١٠- هناك شواهد على ان استخدام الإنترنت من المنزل ، من شأنه أن يجعل الوجود من الزاوية الاجتماعية والنفسية يتدهور، وقد ثبت أن مستخدمي الإنترنت يقل عدد أصدقائهم عبر الزمن، ويمضون فترات أقل مع أسرهم، ويعانون ضغوطاً أكثر في حياتهم اليومية، ويشعرون بالعزلة والاكتئاب.(٣٦).

١١- النصب والاحتيال في عمليات المراهنات والقمار أو في عمليات بيع وشراء وهمية.

١٢- ترويج الشائعات حول المؤسسات والحكومات والشخصيات العامة.

١٣- تنشيط تجارة الدعارة وتسهيل الوصول إلى أماكن ممتهني هذه الرذيلة.

١٤- التهديدات عبر البريد الالكتروني والمضايقة.

١٥- إغراق المستخدم بطوفان من الرسائل التي تدعو إلى مواقع وأنشطة محرمة شرعاً وقانوناً.

١٦- إغواء المراهقين والأطفال.

١٧- ترويج الأفكار العنصرية وبث الكراهية.

١٨- قرصنة البريد الالكتروني للمستخدمين.

١٩- الإيذاء بالتعرض لمعتقدات الناس والتعريض بالشخصيات الدينية.

٢٠- الغزو الفكري للعقائد والتشكيل في الثوابت الدينية والحضارية.

٢١- الشبكة وسيلة اتصالات فعالة للعصابات والمجرمين والحركات الإرهابية.

٢٢- توفر الشبكة جواً مناسباً للترويج للتجارة المحرمة وغسيل الأموال والجرائم المنظمة.

٢٣- هي أرض خصبة تعيش وتنمو فيها شبكات التجسس العالمية وتمارس على مدار الساعة في جمع المعلومات والتجسس على الشبكات ومتابعة الشخصيات الناشطة.

٢٤- عبر الإنترنت تتابع الهجمات الثقافية والحضارية التي قد تزعزع الأمن الفكري والعقدي للشعوب المغلوبة على أمرها وتنشر عبرها القوى الغالية الغالبة فكرها ولغتها وقيمها.(٣٧).

يبقى بين المتفائلين والمتشائمين خيط وصل، ففي الوقت الذي يشير فيه المعنيون بشؤون المجتمع إلى أن هناك مخاطر أمنية من ممارسات بعض الحركات الأصولية المتطرفة (بالمعنى الواسع للكلمة)، غير أنه من الأهمية بمكان أن نسير إلى أن حركات احتجاجية أخرى، وعلى الأخص في مجال أنصار البيئة، بدأت تميل إلى استخدام العنف. ويشهد على ذلك أن العناصر الراديكالية من أنصار البيئة قد تحولت فعلاً للعنف؛ وذلك في الولايات المتحدة الأمريكية وأوروبا الغربية. وعلى سبيل المثال فقد صاغت حركة " الارض الأرض أولاً الديولوجية متماسكة تقوم على العنف".

الواقع أن عديداً من الجوانب السلبية التي يبرزها أنصار الصورة المتشائمة للثورة المعلوماتية، تقوم على مبدأ بالغ البساطة وإن كان بالغ الخطورة من الناحية المعرفية، مؤداه أن الواقع الاقتصادي والاجتماعي والثقافي على مستوى العالم سيبقى كما هو ولن يتغير أبداً!

هذا المبدأ فيه ما فيه من الإيمان بحتمية تاريخية عقيمة فات أوانها بعد أن سقطت الحتمية ذاتها بكل أنماطها في العلم والتاريخ والمجتمع!

إن هذه النظرة المتشائمة تعد نظرة مضادة لمنطق التاريخ الإنساني. لقد سقطت إمبراطوريات مارست الهيمنة ضد البشر قروناً طويلة، وحلت محلها نظم سياسية أكثر انفتاحاً وإنسانية وديمقراطية.

ومن يحلل حالة البشر في القرون السابقة على الثورة الصناعية، بكل ما حفلت به من مجاعات وبؤس وإهدار لإنسانية الإنسان، ويقارنها بالوضع اليوم في عديد من بلاد العالم بعد أن استطاعت الثورة الصناعية تحسين أوضاع البشر، ليدرك أن التقدم الإنساني امكانية فعلية وليس مجرد فرض من الفروض.

صحيح أن دوائر الفقر تزداد في الوقت الراهن على المستوى الكوني، لأسباب شتى، ولكن صحيح أيضاً أن الثورة العلمية والتكنولوجية تفتح آفاقاً واسعة من خلال الهندسة الوراثية، لكي تستطيع الحكومات إشباع الحاجات الأساسية لشعوبها، بتقديم غذاء رخيص، بالإضافة إلى توفير مختلف الخدمات التعليمية والاجتماعية.

إن مجابهة الفقر هي مسؤولية النخب السياسية الحاكمة، والتي يقع على عاتقها إعادة النظر في سياسات توزيع الدخل القويم، لكي لا تستأثر القلة بالقدر الأكبر منه على حساب الطبقات الاجتماعية العريضة المنتجة(٣٨).

فوق هذا وذاك، وبين حالة التقدم التكنولوجي، وحالة الخطر الذي يهدد أمن الناس نتيجة هذا التطور الحاصل في مجال تكنولوجيا المعلومات، يبقى هناك خيط مشترك يربط بين الإيجاب والسلب، يتمثل هذا الخيط في الإنسان، إذ تبقى حالة الأمل معقودة عليه، فهو الذي يمكن أن يجعل من تكنولوجيا المعلومات تجسد جنة النعيم، وهو ذاته يمكن أن يجعل من تكنولوجيا المعلومات تمثل حالة الجحيم، وشتان ما بين الإثنين.

٥- تكنولوجيا الإعلام وتأثيرها على سلوك الأفراد.

أ- تقديم:

بات مؤكداً أنّ هناك اتفاق عام بين المختصين على ان تكنولوجيا التخزين والاسترجاع تشكل مع تكنولوجيا الاتصالات الحديثة، تكنولوجيا المعلومات بمعناها الواسع والشامل.

وتكنولوجيا الإعلام تعني تكنولوجيا الاتصال، والأخيرة أصبحت تمثل العمود الفقري للعمل الأعلامي، ولهذا وذاك، فإن أمر دراسة تأثير الجانب السلبي (المخاطر الإعلامية) لتكنولوجيا الإعلام بات ضرورياً، بل أمراً لابد منه.

يكاد يكون هناك إجماع على إن الإعلام في العصر الراهن أصبح يحتل مكانه حيوية، بل رئيسة بين وسائل الحياة المتعددة في عالمنا المعاصر، بل يمكن القول: إن وسائل وأنشطة الحياة الآن، كالتعليم والصحة والصناعة والتجارة، تعتمد اعتماداً رئيسياً على الأعلام لتيسيرها ورواجها. وإذا شئنا أن نتصور حجم هذه الأهمية، فيكفينا تخيل حال المجتمعات المعاصرة بغير أعلام، فلا يوجد الآن مجتمع متقدم أو نام يمكنه مواجهة المتطلبات المعاصرة من النمو والتنوع بغير وسائل اتصال مؤثرة وسريعة ومتنوعة.

ب- كيف تستحوذ المعلوماتية الإعلامية على المجتمع؟

إن التقدم التكنولوجي صاحبه شعور الإنسان بأن الآلة تهدد القيم الروحية للجنس البشري ومن ثم ظهرت العداوة بين الإنسان والآلة ومعظم الهجوم الذي يوجهه اليوم لفكرة التقدم التكنولوجي لا تأتي من الدوائر الاقتصادية، ولكنها تأتي من الجماعات التي تهتم بالقيم الثقافية والروحية، والاعتقاد المسيطر على هذا النقد يتمثل في اعتقاد النقاد بأننا قد صرنا ضحايا التطور التكنولوجي على حساب الإنسان(٣٩).

تنبع خطورة المد المعلوماتي الجديد من قدرته على استحواذه على القنوات والأدوات التي تصنع ثقافة الفرد وبالتالي تستحوذ على بنيته المعرفية وتتحكم في سلوكه وتوجهاته وأهدافه، وبعبارة موجزة فإنها تسترقه في القطيع الإلكتروني التي يقوده قلة ونخبة تستحوذ على معظم موارد العالم. والثورة المعلوماتية هي من أخطر التحديات والأعاصير التي تهب علينا وتجتاحنا من جذورنا لتقيدنا في زنزاناتها الإعلامية والتقنية وتغسل عقولنا بإعلاناتها وتأثيراتها الضوئية المبهرة حتى تمحي صورنا المعرفية الأصلية وتؤسس في أعماق حضارتنا معرفيتها الهزيلة القائمة على المادة واللهو والأنانية.

إن أساس ظهور المعلوماتية وتحولها إلى قوة العصر يرتكز أساساً على تطور تقنيات الاتصال وسرعتها بحيث أصبحت لها السلطة في صناعة الأحداث، وبناء السياسات وإسقاط الأنظمة، وتوتير الاقتصاد، وانهياره، والتهام الثقافات، وتعليب العقول، وللمعلوماتية عبر أدواتها الاتصالية وإخطبوطها الإعلامي القدرة على صناعة الواقع الوهمي حسب توجهات النخبة المسيطرة

الاقتصادية والفكرية للاستئثار والتحكم والسلطة، ذلك أن القدرة على رسم حدود الواقع هي القدرة على السيطرة، وأن عملية نقل المعلومات هي السلطة واستئثار فئات معينة بحق الوصول أو التعامل معها يمثل نوعاً من السلطة خطراً وعنيداً.

فالسلطة المعلوماتية هي القدرة على استثمار سرعة الاتصالات لإيصال معلومات مجهزة مسبقة لأهداف معينة وهنا تكمن جوهر ظاهرة المعلوماتية باستغلال الفراغ الذي يخلفه متلقي الرسائل بالاتصال السريع عندما يفقد الوقت اللازم لاستيعاب الرسالة وهضمها.

لا شك أن الاتصالات هي عصب عصر المعلومات وعملية الاتصال تتطلب في الأساس مُرسِلا ومُرسَلا إليه وقناة اتصال ومن شأن اعتماد وسائل الاتصال البالغة السرعة أن تجعل المعلومات تنتقل عبر قناة الاتصال في فترة وجيزة جداً تؤدي إلى وضع المرسل والمرسل إليه وجهاً لوجه وبالتالي انهيار عولمة المعلومات التي عرفها المختصون بأنها: الوقت الذي تستغرقه المعلومات في قناة الاتصال. فتقنية الاتصالات وسرعتها وقدرتها على إيجاد التواصل المادي بين البشر وضعتها في مقدم الأولويات الثقافية والاقتصادية، بحيث أصبحت المنبر الثقافي والتعليمي الذي يكتسب منه الناس حتى أصبح ممتلكوا هذه الوسائل المعلوماتية هم الذين يصنعون المعلومة ويرسمون واقعاً خيالياً يتحكمون بتأثيراته على المتلقي المسكين، ففي ثقافة التلفاز مثلاً، كثيراً ما يعتقدون المرء أن ما يراه هو حق وهو في الغالب أكثر أهمية من الحقيقة الفعلية حين يمس الأمر فهم وتصورات النشاطات الإنسانية، ففي الأفلام صار الناس لا يميزن بين ما هو تاريخي حقاً وما هو روائي، فقد غدا الإعلام ديناً مدنياً حل محل التاريخ والثقافات القومية والعائلة والأصدقاء، وبات القوة السائدة التي تخلق تصوراتنا العقلية عن الواقع ، والإعلام ببساطة يصنع ويجهز ما يباع أي كل ما يزيد الأرباح وما يباع هو الإثارة والجذب السريع والفوري. (٤٠)

وفق المعطيات السابقة تتضح أين تكمن خطورة تكنولوجيا الإعلام، لاسيما تكنولوجيا الاتصالات، إذ تعيش المجتمعات اليوم في حالة فقر مدقع ليس على الصعيد الاقتصادي فحسب، بل فقر على جميع الأصعدة، الثقافية منها، والمعرفية ، والنفسية والاجتماعية... الخ، مما جعل من تكنولوجيا الإعلام الحديثة ووفق إمكانياتها المتاحة حالياً تصنع جيلاً، بل تؤسس لمجتمعات جديدة تسييرها مثلما يُريد ممتلكوا هذه التكنولوجيا، وهذا يمثل قمة خطر هذا النوع من التكنولوجيا.

وسائل الاتصال السريع هذه لا تؤدي فقط إلى عملية تسهيل أعمال المستخدم ورفاهيته، بل أنها تصنع له ثقافته الخاصة وسلوكه بجميع نواحيه وبرنامجه اليومي الخاص حتى ذوقه في الشرب

والأكل، وبل وتسيطر عليه كاملاً عندما تحدد له ما هو الصحيح أو الخطأ والحق أو الباطل، فهوليود مثلاً ، لا تنتج أفلاماً فحسب بل تولد قوة ونفوذاً ، إنها تساهم تحديداً في تظهير صورة الخير والشر في العديد من الأوضاع الإستراتيجية.

يمكن أن نعطي مثالاً على ما سبق إذ باتت الـ CNN التي قالت عنها (مادلين أولبرايت) بأنها العضو السادس في مجلس الأمن الدولي - رمزاً للإعلام الذي لم يعد مجرد وسيلة نقل ولكن أصبحت مصدراً للمعلومة، وباتت قادرة على صياغة رؤية خاصة للعالم تدخل إلى لا وعي المشاهدين: الرؤية الأمريكية. وإذا كانت الماكنة المعلوماتية قادرة على تحويل الواقع إلى خيال وتغيير الخيال إلى واقع أو الشر إلى خير ، فإن الأمر سيصبح خطيراً حينئذ باعتبار أن أدوات المعلوماتية أصبحت العصب الحيوي الذي يتنفس منه العالم كافة أفكاره وتحركاته وفعالياته، فلقد أصبحت ألعاب الواقع الافتراضي في طريقها لتصبح أكثر من مجرد وسيلة للترفيه إنها تتحول إلى جزء حيوي، من الثقافة الجديدة لدى الشباب ، ما الذي سيفعله مدمنوا الألعاب إذا ما اشتد عدوهم؟

إن مبعث الخطورة ينبع من كون أدوات المعلوماتية هي في يد قلة من الأباطرة الذين احكموا سياساتهم ونفوذهم ويفرضون ما يريدون على العالم، فشرطة مثل (T and AT) التي تعتبر إحدى أكبر شركات الاتصالات البعيدة المدى في العالم تقدر أن ثمة ألفين أو ثلاثة آلاف شركة عملاقة تحتاج على خدماتها العالمية، ويوجد حسب إحصاءات منظمة الأمم المتحدة (٣٥) ألف شركة كبيرة عابرة للأوطان ترتبط بها (١١٥٠) ألف شركة تابعة، وقد اتسعت تلك الشبكة بحيث يقدر أن المبيعات ما بين الشركات التابعة التي تنتمي للمجموعة نفسها صارت تمثل ربع التجارة العالمية، وهذه البنية الجماعية التي تشهد عز نموها لم تعد مرتبطة بأحكام الدولة والأمة وهي تمثل عنصراً أساسياً من نظام الغد العالمي. (٤١)

لقد فتحت ثورة المعلومات آفاقاً واسعة أمام البشر للعثور على رؤى جديدة عجز عنها السابقون لافتقادهم لتلك التقنيات، بيد أن السؤال القلق والذي يبحث عن إجابة واقعية مفاده: كيف يستطيع الإنسان أن يتعامل مع هذا الاجتياح المعلوماتي بشكل موضوعي وعقلاني ونقدي؟ وما الذي سيفعله الشخص العادي وهو يجد نفسه ليس في مواجهة (٥٠) قناة فقط، بل آلاف من أفلام السينما والعروض المختلفة؟ وكيف سيواكبون مئات القنوات من التلفاز التفاعلي وخدمات السوق وكلها تتزاحم لجذب انتباهه؟ وكيف سيختارون المنتج الصحيح من أحسن بائع وبأرخص الأسعار؟

تلك أسئلة تبحث عن إجابة نابعة من الواقع الفعلي للمجتمعات الإنسانية . ويمكن توضيح ذلـك مـن خـلال رصد ملامح الثورة المعلوماتية في الجانب الاتصالي، فمن ملامح هذه الظاهرة (أباطرة المعلومـات)، فقـد ظهـر في خـضم هـذه الأعاصير المعلوماتية رجال من نتاجـات الرأسـمالية النفعيـة أصبحوا يـسيّرون العـالم بـصناعتهم للأحـداث وتـسويقهم التجاري للمعلومات عبر احتكارهم لأساطيل كبيرة من أدوات الإعلام والمعلومات، مثل (بيـل غيـتس) ، الـذي يعـد أغنـى رجل في العالم، وصاحب أكبر شركة كمبيوتر أنتجت نظام تشغيل تعتمـد عليـه معظـم الأجهـزة الكومبيوتريـة في العـالم، ومثل (روبرت مردوخ) ذلك اليهودي الأسترالي المتجنس بمجموعة جنسيات عالمية الذي بـدأ حياتـه العمليـة عـام (١٩٥٢) وكان عمره وقتها (٢١) عاماً حين ورث عن أبيه جريدتين محليتين في أستراليا، لكنه انطلق مثل الصاروخ ليـصبح إمبراطـور الإعلام العالمي حين سيطر على (٧٠%) من الصحف الأسترالية ، وبدأ منذ عام (١٩٦٩) بالتوجه إلى بريطانيـا حيـث اشـترى صحف (التايمز والصن) ثم أصدر (صنداي تايمز وينوز أوف ورلد) ثم سيطر على محطة (بي سكاي) التي تضم (٤٠) قناة، ثم محطة (جراند سكاي) التي تضم (٧) قنوات ثم (بريميوم شانلز) واتجه بعد ذلك إلى كـل العـالم، ففـي اليابـان يمتلـك محطة (جي سكاي ين) وفي الصين قناة (فونيلس) ، وفي الهنـد قنـاة (إل سـكاي بي)، وفي إندونيـسيا (تلفـاز إندونيـسيا)، وقناة في جنوب أفريقيا، وقناتان في البرازيـل والمكـسيك، وفي أمريكـا يمتلـك مجموعـة قنـوات فـوكس القـرن العـشرينن وفوكس ٢٠٠٠، حيث يسيطر على ٢٢قناة تغطي (٤٠%) من مشاهدي التلفاز في الولايات المتحـدة الأمريكيـة، إضـافة إلى امتلاكه لجريدة (الواشنطن بوست) ودا نشر (هابرر كولينز).

وفي استراليا فإن إمبراطورية (مردوخ) قد توقفت إلى (٢٦٩) جريدة يومية ومحطة تلفازية بها (٣٤) قنـاة. وقـد قـال عنه (تيد ترنر) أحد أباطرة المعلومات أيضاً وصاحب الـ (CNN) لا تسمحوا بدخول هذا الرجـل عـلى بلـدكم، فهـو يريـد السيطرة على جميع محطات التلفاز في العالم ويريد التأثير على كل الحكومات.

إذ كان روبرت مردوخ يريد السيطرة والتأثير عـلى الحكومـات والتـي مـن المفـروض تمتلـك الحمايـة الكافيـة -أي- الحماية الثقافية والفكرية والسياسية ... الخ، فإن الشعوب وفق ذلك تكون أكثر عرضة للسيطرة والتـأثير، وبالتـالي يمكـن تغيير ميولهم الثقافية والفكرية...

وعلى ذكر السيطرة والتأثير، يذكر صاحب كتب احتكار الإعلام، أن طبقة تمثل (١%) من الناس تمتلك الـسيطرة عـلى الإعلام، ففي عام (١٩٨٣) كانت أغلبية ملكية الشركات محصورة

في خمسين شركة، وفي عام (١٩٩٧) تقلصت الشركات المسيطرة على الإعلام إلى عشر شركات ، وعندما يسيطر مجموعة قليلة من الأشخاص هم رؤساء شركات على أكثر من نصف المعلومات والأفكار التي تصل إلى (٢٢٠) مليون أمريكي، ومن خلال امتلاك الإعلام والسيطرة عليه، فإن ما يتراوح بين (٣٠) إلى (٥٠) مصرفاً وما يتروارح بين (١٠) على (٥٠) شركة إعلامية يسيطرون على العالم ويصنعون أو يحطمون السياسيين والحكومات.

لم تتوقف ملامح الثورة المعلوماتية في الجانب الإعلامي عند هذا الحد، بل إن أحد أهم ملامحها الخطيرة هي الاندماج الثقافي والندثار اللغات، إذ أن أحد ملامح ظاهرة المعلوماتية هو ذلك التداخل الذي أفرزته وفرة وسائل الاتصال، وسرعتها، حيث استطاعت الدول القوية بأدواتها وخبرتها ومنسوجها الثقافي أن تغزو الشعوب الضعيفة التي تفتقر لقوة الثقافة وأصالة التفكير وروح الثقة بعناصر حضارتها لتذوب في عناصر الثقافات القوية وتعيش مفتخرة على هوامش المجتمعات المعولمة.

واللغة هي أحد أهم المفردات التي تفرضها الثقافة الغازية على المجتمعات المستأصلة لتصبح مفرداتها عنواناً رئيساً في كثير من العناوين الرئيسية، وتفقد اللغات الضعيفة التي لا تستند إلى ثقافة أصيلة ونسيج ثقافي متماسك وجودها وتصبح من اللغات الميتة ، والخطير في الأمر أن اللغة تصبح مفتاحاً لدخول العالم الجديد ومظهراً للتقدمية الشكلية لا سيما عندما تفقد المجتمعات إيمانها بثقافتها وتتصل من أصالتها هروباً من واقعها المتخلف، فاللغة ليست مجرد آلة وسيلة للتخاطب وإنما بالدرجة الأولى آلة للتفكير والتقدم.

إن اللغات الأخرى لا تمثل خطراً بعد ذاتها ، بل تعلمها والاستفادة منها بشكل منطلقاً مهماً لزيادة الخبرة واستثمار العبر من تجارب الآخرين ولكن الخطورة في الأمر أن تتحول اللغة إلى ثقافة بديلة تحل نفسها في الشخصيات المهزوزة التي فقدت قابليتها الذاتية وأصالتها الحضارية.

يعتقد (ادوارد هوف) الخبير باللسانيات بجامعة ساوثرن في كاليفورنيا، أن الكومبيوتر سيقود العالم إلى تهديم برج بابل اللغوي الذي لا يزال عائقاً أمام البشرية، حيث ستمكن من خلق أجواء التفاهم بين الإنسان والآلة ، وتوليد الآلة لمعارف ينهل منها الإنسان، ويضيف قائلاً: إن تاريخ العالم يشير إلى أن الناس يضطرون إلى تجزئة لغتهم وخلق اللهجات؛ لأن اللغات لدى نضوجها أو شيخوختها تزداد تعقيداً وتنوعا، ومع حصول التماذج الحالي في اللغات على المستوى العالمي خصوصاً مع توسع الشبكة الإلكترونية والبريد الإلكتروني، فإن اللغات ستزداد امتزاجاً ويؤدي

تطوير برامج كومبيوترية للترجمة الآلية الدقيقة إلى بروز حرية الاختيار كأحد أهم ملامح النشاط اللغوي للإنسان لتسجيل أفكاره وتحويلها على (٧) آلاف لغة وسيهدد ذلك اللغة الإنجليزية التي لا تزال اللغة الطاغية في الإنترنت.

تشير التوقعات إلى احتمال اندثار ما يربو على نصف اللغات التي يعتقد أن عددها يصل إلى (٦) آلاف لغة في العالم، وتتوقع (روزماري اوستلر) الباحثة الأمريكية في اللغات أن منتصف القرن الحالي سيشهد حلول هذه الظاهرة بسبب هيمنة عشر من اللغات أو أكثر على النشاطات البشرية، وقد تقود هذه الظاهرة إلى تدمير بعض الجوانب المهمة في ثقافات العالم العظيمة كما أن اللغات الأصيلة تمثل جزءاً مهماً من تراث الشعوب.(٤٢)

إذا كان الأمر كذلك، فإن هناك العديد من الشعوب الضعيفة التي سحقت سابقاً بفعل الاستعمار وقوة سلاحه، فإنها اليوم ستسحق مرة أخرى بقوة السلطة المعلوماتية والإعلامية، بمعنى آخر أضحت تكنولوجيا المعلومات معول هدم لتدمير ما بنته الشعوب الضعيفة طيلة الفترة الماضية، وهذا خطر ما بعده خطر ينتظر هذه الشعوب ودولها ، تمثله تكنولوجيا المعلومات.

جـ- تكنولوجيا الاتصال وتأثيرها على سلوك الفرد والمجتمع.

مما لا شك فيه أن نسبة الاختلاف من حيث التأثر تختلف من بيئة إلى أخرى، ومن فئة عمرية إلى أخرى، ومن شعب إلى آخر، وذلك كله راجع إلى مستوى الوعي المعرفي والثقافي لكل فرد وشعب. ومن هنا يمكن القول: إن ظاهرة تأثير وسائل الاتصال على أفراد المجتمع باتت واضحة، لاسيما التلفاز، إذ أن وسائل الاتصال باتت تحاصر المواطن من كل حدب وصوب وعلى مدار الليل والنهار.

إن كل عملية إعلامية ترتبط ارتباطاً وثيقاً بفكرة الاتصال، فما دام هناك إعلام فهناك بالضرورة عملية اتصال، وتتكون عملية الاتصال من عناصر عدة هي: المرسل والرسالة.
وقناة الإرسال والمستقبل، وتتوج عملية الاتصال بما يسمى برجع الصدى أو المعلومات الراجعة (Feed back). وذلك حسب المعادلة التي وضعها (Harold laswell) في سنة (١٩٤٨) والمتمثلة في من يقول ماذا ، ولمن ، وبأي وسيلة وما النتائج المترتبة على ذلك؟ وحسب هذا المنظور، فإن المرسل، تمشياً مع الهدف الذي يريد الوصول إليه يكون رسالة من شانها التأثير في الآخرين وفق المعطيات السابقة ، تسير الرسالة داخل قناة ثم يتلقاها المستقبل بحيث تؤثر فيه أما بالسلب أو الإيجاب. ومن أهداف الاتصال: تقديم المعلومات ومحاولة الإقناع، وتغيير الرأي، وطلب القيام بعمل ما والقيام

بعملية تعليم، والتأثير على التوازن العاطفي والصحة النفسية وإثارة الشعور. وهذه الأهداف كلها تؤثر على محتوى الرسالة وطرائق الاتصال.

تتنوع وسائل الاتصال بتنوع الرسالة والأهداف والمكان والزمان، بالإضافة إلى الاتصال اللفظي - السمعي مثل الخطابة والمحاضرات والراديو، فهناك التلفاز والفيديو والسينما والصور المتحركة والكتب والمجلات والمسرح والحاسوب..الخ.(٤٣).

تكمن خطورة تكنولوجيا الإعلام في العالم إنها تبث من طرف واحد، الطرف الذي يمثل جانب القوة والتقدم التكنولوجي، وهنا تتمثل خطورة البث الإعلامي، حيث يبث الجانب القوي ما يحلو له، وفي أحيان كثيرة يريد أن يوصل رسائله مقصودة ومعينة، وهذا يمكن نطلق عليه الهيمنة الإعلامية للدول المتقدمة على الدول النامية، وتتمثل تلك الهيمنة في تحكم الدول الكبرى بواسطة إمكاناتها الهائلة، ووكالات أنبائها، وتقدمها العلمي والتكنولوجي في مجال الاتصالات وفي مجال المعلومات والأخبار ولاسيما البرامج التليفزيونية التي تأتي معظمها من مصادر غربية بصفة عامة، ومصادر أمريكية خاصة.

إن وكالات الأنباء العالمية الكبرى، وكالات أجنبية، أربعة منها تابعة للغرب، والخامسة تابعة للإتحاد السوفياتي السابق، وهذا الأمر له خطورته من حيث إمكان قيام تلك الوكالات ببث ما تريده من أخبار وبرامج لتحقيق أهدافها إلى جانب ضعف القدرة في الدول النامية على تحليل ومتابعة ما وراء تلك الأخبار والبرامج، وتحديد أهدافها المباشرة وغير المباشرة ومن ثم التصدي لحماية مجتمعاتها من تلك الآثار المدمرة الناتجة عن تلك الهيمنة الإعلامية، إن العالم اليوم كما تقول إحصائيات اليونسكو بتسلم (٨٠%) من الأخبار عبر لندن وباريس ونيويورك .(٤٤)

عندما يكون البث من طرف، وهو الطرف المتقدم تكنولوجيا، وعندما يكون الطرف المتلقي لا يستطيع منع كل أو جزء من هذا البث، تكمن هنا خطورة الإعلام التكنولوجي، ووفقاً لذلك، ستبقى المجتمعات المتخلفة تكنولوجيا عرضة لغزو استعماري جديد، يتمثل في الاستعمار الثقافي، وهو الأخطر من كل أنواع الاستعمار الأخرى. لقد أثبتت العديد من الدارسات والبحوث الغربية أنه لا يوجد في عالم اليوم أي مجتمع يتمتع بالحصانة ضد تأثير وسائل الإعلام الأمريكية، بل أن الباحث الأمريكي (وليام ريد) يقول: إن وسائل الإعلام الأمريكية قد أصبحت فعلاً قوة مؤثرة في النظام الاجتماعي العالمي، ويعزى الباحث أسباب هذه الظاهرة إلى

مدى انتشار وسائل الإعلام الأمريكية. لاسيما تغلغلها في الدول النامية، إلى الحد الذي أصبحت معه هذه الدول معتمدة اعتماداً شبه كلي على الولايات المتحدة بوصفها مصدر للمواد الإعلامية.

لم يكن تفسير الباحث (وليام ريد) لهذه الظاهرة منفرداً أو وحيداً، بل أيّده في طرحه السابق عدد من الباحثين المختصين، ويأتي في مقدمتهم (جيرمي تنستل) و (هيلبرت شبلر) و (أنتوني سميث) و (ألف ويلز) وغيرهم، بل أنهم اعتبروا تلك الهيمنة لوسائل الإعلام الغربية على المجتمعات النامية، قد بدأ ينظر إليها على أنها نوع من "الاستعمار الثقافي"، الذي يعادل في مفهومه للاستعمار السياسي القديم، والاستعمار الاقتصادي.

علماً أن أول من نبّه إلى خطورة الغزو الثقافي الأمريكي الباحث الأمريكي (هربرت شيلر)، الذي اتهم وسائل الإعلام الأمريكية بمحاولة فرض نوع من الاستعمار الثقافي على دول العالم النامي، وقد ركز شبلر في أبحاثه على مدى خطورة وسائل الإعلام الأمريكية على الثقافات الوطنية المميزة للمجتمعات النامية. ويقول شبلر: إن تأثير وسائل الإعلام الأمريكية يؤدي إلى "أمركة" الثقافات المحلية في الدول النامية عن طريق هيمنة الشركات الأمريكية الكبرى على السوق التجاري العالمي وعلى شبكة الأقمار الصناعية للاتصالات.

أيد نظرية شبلر حول "الاستعمار الثقافي الأمريكي" عدة باحثين غير أمريكيين وعلى رأسهم الباحث البريطاني (جيرمي تنستل)، ويقرُّ الأخير بهيمنة وسائل الإعلام الأنجلو - أمريكية على وسائل الإعلام الدولية. وقد حذرت لجنة "مكبرايد" (شين مكبرايد) الإيرلندي الجنسية والحائز على جائزة نوبل للسلام والذي ترأس اللجنة التي كانت تحت إشراف وتمويل منظمة اليونسكو، حذرت من أخطار الغزو الثقافي الذي يأخذ شكل التبعية لأنماط الحياة والقيم الغربية المستوردة والتي تهدد الذاتية الثقافية للدول النامية.(٤٥)

إذا كانت الهيمنة الإعلامية تبث رسائل إعلامية موجهة لدولة أو لإقليم معين، فإن المشكلة تكمن هنا والخطورة تأتي في أحيان كثيرة ضمن هذه البرامج الموجهة، لاسيما إذا كانت قادمة من مجتمع تنتشر فيه الجريمة، مثل الولايات المتحدة الأمريكية والخطورة تتجسد هنا في تهيئة الفرد والمجتمع من الناحية النفسية.

على الرغم من أن الجريمة والانحراف يعتبران ظاهرتين معقدتين لهما علاقة بالتكوين النفسي والاجتماعي والعقلي والثقافي للفرد، إلا أن الكثير من الدراسات والبحوث الميدانية أثبتت أن وسائل الاتصال تلعب دوراً مهماً في حدوثهما كذلك. فقد أجريت أكثر من ثلاثة آلاف دراسة

لقياس أثر وسائل الاتصال على العنف ضد الأشخاص والأعمال الإجرامية والانحرافية والأفعال اللا اجتماعية. فعلى الرغم من استمرار الجدل حول أثرها، فإن معظم الآراء تجمع على وجود علاقة بين مشاهدة العنف والسلوك العدواني.

قام الأستاذ (Bradon Centerwall) في دراسة مشهورة بجامعة واشنطن، توصل الباحث إلى النتيجة التي مفادها أنه إذا لم يكن هناك تلفاز لكان معدل الجريمة في أمريكا أقل مما هو عليه الآن بمقدار (١٠.٠٠٠) جريمة قتل كل سنة، ومعدل الاغتصاب أقبل مما هو عليه بـ (٧٠.٠٠٠)، ومعدل الإعتداء المؤدي إلى الجروح أقل مما هو عليه بـ (٧٠.٠٠٠)، ومعدل الجريمة بصفة عامة ينخفض إلى النصف من هو عليه الآن.

إن الطريقة التي تصور بها وسائل الاتصال الجريمة والعنف تشكل ردود أفعال أو سلوكيات غير ملائمة من قبل المشاهدين أو المستمعين أو القراء، وهذا يأخذ أشكالاً متعددة منها تزايد الخوف من الجرائم وتزايد اقتراف الجرائم في حد ذاتها. ولقد وجدت بعض البحوث الأخرى وعلاقة بين المشاهد العالية للتلفاز والخوف من الجرائم، كما كشفت بعض الدراسات الأخرى النقاب عن مدى تأثير وسائل الاتصال على اقتراف السلوك المنحرف. فعلى سبيل المثال، وجدت الدراسة التي أجراها (Hartnagel) وآخرون سنة (١٩٧٥)، علاقة بين الإعلام الذي يقدم المشاهد العنيفة وبين السلوك العنيف لطلبة المدارس الثانوية.

كما قارن (Belson) عام (١٩٧٨)، السلوك العنيف لمجموعتين من الأطفال، أو لهما معرضين كثيراً لمشاهدة المشاهد العنيفة في التلفاز والسينما، والثاني قليل التعرض لمثل هذه المشاهد. حيث وجد أن الأطفال الأكثر مشاهدة لأفلام العنف يميلون إلى إرتكاب أفعال أكثر عنفاً من الأفعال التي يرتكبها قليلوا المشاهدة للأفلام العنيفة. وهذه العلاقة تصدق كذلك بالنسبة للأفلام التي تصور العلاقات الشخصية العنيفة واستعمال العنف غير المبرر والعنف الموضوعي المقبول. بينما كشفت الدراسة على العكس من ذلك أن مشاهدة العنف الرياضي والصور المتحركة وعلم الخيال والأفلام الهزلية التي يتخللها عنف حفيف ليس لها نفس التأثير على المشاهدين الشباب.

هناك دراستان أخريان أجراهما (Phillips) عام ١٩٨٢-١٩٨٣، فحص من خلالهما أثر الإنتحارات الخيالية والمنازلات الرياضية العنيفة مثل الملاكمة على العنف الشخصي. فتعرضت دراسته الأولى إلى عدد الانتحارات المتأثرة بالانتحارات الخيالية التي تحدث في المسلسلات التلفازية (soapoper) فوجد أن عدد الانتحارات تكثر بعد الانتحارات التي تحدث في الأفلام. وكذا الحال

وجد أن المحاولات الانتحارية ترتفع بفعل التصوير الإعلامي. وهذه الانتحارات تكثر بصفة خاصة بين نساء الحضر اللاتي يشبهن في تجاربهن وحياتهن الشخصيات التي تظهر في المسلسلات التي تقدّم بعد الظهر.

أما دراسته الثانية، فقد فحصت مدى العلاقة بين جرائم القتل وتقديم المنازلات العنيفة بين الأوزان الثقيلة، فوجد زيادة ذات دلالة في عدد جرائم القتل بثلاثة أو أربعة ايام بعد هذه المنازلات. ويتزايد أثرها إذا ما تعلق الأمر بالمنازلات الأكثر دعاية وأن ضحايا هذه الجرائم يشبهون في سماتهم المنازلين الخاسرين.(٤٦).

لا يقتصر أثر وسائل الاتصال في إثارة العنف عند الصغار، بل يكون أثره أكثر عند الكبار كذلك. وهذا راجع كما يعتقد (Andisin) إلى مدة مشاهدتهم الأطول من مدة مشاهدة الصغار نظراً لفرق السن. حيث أجرى هذا الأخير عدة دراسات مخبرية وميدانية واستمرت العلاقة في كل منها بين مشاهدة التلفاز والعدوانية. وإذا كان التلفاز حظي باهتمامات الباحثين، فإن أنواع الاتصال الأخرى، حظيت بالاهتمام نظراً لما تحدثه من أثر على الانحراف، حيث أجمعوا على أنها هي الأخرى لها علاقة مباشرة بالعنف الجنسي ضد النساء. ففي سنة (١٩٨٦) أكدت اللجنة المؤلفة من المدعين العامين لدراسة أثر الأفلام والصور الخليعة أن هناك علاقة متينة بين هذا النوع من الصور والأفلام والعدوانية، وقد راجعت هذه اللجنة كل البحوث التي أجريت حول هذا الموضوع منذ السبعينيات وكانت خلاصتها أن هناك علاقة مباشرة بين نوع المادة الخليعة التي تقدمها وسائل الاتصال والعدوانية.

يتضح مما سبق أن التلفاز ووسائل الاتصال الأخرى تصور العنف كخيار وحيد متاح لحل الصراعات في الوقت الذي تعزز فيه سلسلة المشاهد العنيفة الحلول السلبية والمداخل المحدودة في حل المشاكل.. بالإضافة إلى ذلك، فإن هذه السلسلة من المشاهد العنيفة ترفع من مستوى هيجان النظام العصبي لدى المشاهد. وقد وجد العلماء الاجتماعيون بان مستوى الهيجان العصبي يؤثر على غدد الغضب والأفعال العدوانية. حيث إن المشاهد مثل المدمن على المخدرات دائماً يطلب المزيد من الإثارة للوصول إلى أعلى مستوى من الهيجان. فهو يشبه إلى حد كبير المدمن من حيث إنه لا يصبح فقط متسامحاً مع العنف في وسائل الاتصال، ولكنه يصبح أيضاً متسامحاً معه في الحياة الواقعية. (٤٧)

بشكل عام يمكن القول: إن تأثير وسائل الإعلام، لاسيما السينما والتلفاز في مجال الجريمة والمجرم، يمكن أن نرمز له بثلاثة كلمات يجمع بينها نسق لغوي وحركي متشابه، وهي كلمات "تمهيد" ، و"تمجيد"، و" تقليد".

أما التمهيد، فيقصد به أن عرض أفلام ومسلسلات تحتوي على الإثارة والعنف والجنس والقتل والتذمر والتخريب (الكاراتيه والمصارعة الحرة وغيرها) .. الخ. إنما يؤدي إلى "تمهيد" نفوس المشاهدين. إلى أن تلك الأشياء عادية ويمكن حدوثها (وليست مستحيلة). أي تؤدي إلى وجود صلة بين تلك الأمور الغريبة وبين نفوس المشاهدين أو متلقي المواد الإعلامية وفي ذلك خطر، وقد لا يمكن تلمسه بوضوح خلال فترة التمهيد هذه إلا أنه يمكن الإحساس بمدى هذا الخطر في المراحل الأخرى.

أما التمجيد، فيقصد به "الحبكة الفنية" إذا صح هذا التعبير هنا، وعوامل التسويق التجاري وتحقيق أعلى الإيرادات وأقصى الأرباح، ومحاولة ادعاء التجديد ومعدوا المسلسلات، يحرصون في معظم الأحيان على إحاطة "المجرم" أو بطل الفيلم أو المسلسل بهالة من "التمجيد" لذكائه وقدرته وعبقريته، صحيح أنهم خوفاً من احتمال رفض أعمالهم الفنية وتعرضهم نتيجة لذلك لخسارة مادية، يحاولون في آخر لحظات الفيلم أو المسلسل أن يضعوا نهاية مأسوية لهذا البطل أو "المجرم" تثبت أن الجريمة لا تفيد، لكن تلك اللحظات لا تستطيع أن تلغي هذا التمجيد الذي استمر طوال الفيلم أو طوال حلقات ممتدة من المسلسل، ولن تستطيع تلك اللحظات في نهاية الفيلم، أن تحول أو تغير هذا "التعاطف" الظاهر أو الخفي مع المجرم والجريمة الذي غرسه الفيلم أو المسلسل في نفسيته، بل وفي العقل الباطن وفي منطقة، اللاشعور لدى المشاهد.

أما التقليد، فهي النتيجة المتوقعة لعاملي " التمهيد" و "التمجيد" السابقين؛ وذلك أن بعض الأفراد المتلقين بوسائل الإعلام في غيبية عوامل كثيرة، كضعف التوعية الدينية والأخلاقية، وضعف الرقابة العامة والخاصة لكل من الدولة والأسرة والمدرسة سنقول – نقول: إن هؤلاء الأفراد سيجدون إذا سنحت لهم الفرصة وتهيأت لهم أن "يقلدوا" ما قرأه أو شاهدوه بوعي أو بدون وعي، حتى يشعروا نفسياً بذلك التمجيد ولو أمام أنفسهم، قبل أن يحصلوا على فوائد معنوية أو مادية من تقليدهم لها شاهدوه من جرائم ، فما بالنا إذا كان المقلدون من الأطفال.(٤٨).

بشكل عام، اتهمت وسائل الإعلام المختلفة بأنها مسوؤلة عن:

١- تدهور مستوى الذوق الثقافي العام.

٢- زيادة معدلات اللامبالاة والميل إلى انتهاك القانون.

٣- المساهمة في الإنهيار الأخلاقي العام.

٤- تشجيع الجماهير على السلطة السياسية.

٥- قمع القدرة على الخلق والابتكار. (٤٩)

٦- تعلم الأفراد أساليب جديدة لارتكاب الجرائم، وخير مثال على ذلك هو ما تنشره الصحف بين حين وآخر عن أحدث الوسائل الفنية لسرقة السيارات، وكيفية تغيير معالم ملكيتها الحقيقية، وطرق تزوير وثائق تسجيلها إلى غير ذلك من الوسائل المستحدثة في عالم الجريمة.

٧- درجت بعض وسائل الإعلام على نشر أخبار الجريمة بطريقة اعتيادية، الأمر الذي قد يجعلها حدثاً مألوفاً بالنسبة للقارئ، وفي ذلك الضرر ما لا يخفي.

٨- تقوم بعض وسائل الإعلام بإظهار جدوى الجريمة في نهاية المطاف فهي تبرز أحياناً كيف يعيش بعض المجرمين المحترفين، وكيف يسرفون في متع الحياة.

٩- تميل بعض وسائل الإعلام إلى إظهار المجرم في صورة البطل الأمر الذي يجعل منه نموذجاً حياً لأكثر من طفل أو مراهق أو بالغ، وتصبح بالمقابل الأجهزة المختصة بملاحقة المجرم محل سخرية واستهزاء.

١٠- تعيق بعض وسائل عمل الأجهزة المختصة من خلال ما تنشره من معلومات عن الخطط والتحقيقات فتفسد عملها وتسدي بغير قصد إلى المجرمين خدمة كبرى.(٥٠)

١١- تسهل أحياناً بعض وسائل الإعلام فكرة الجريمة أو وسيلة تنفذها أو أسلوب إخفائها.

١٢- تثير بعض الغرائز والرغبات الكافة في نفوس بعض المراهقين وكذلك الكبار لاسيما المنحرفين.

يتضح مما سبق، إن التحدي المطروح على الساحة العالمية اليوم، ونحن نعيش البدايات الأولى من القرن الحادي والعشرين، هو بلا أدنى شك، تحدي تكنولوجيا المعلومات. وبين حالة التحدي، والهم والقلق، والحذر والترقب، والخطر الذي يحدق بالمجتمع المعلوماتي العالمي، من كل حدب وصوب، يبقى الأمل معقوداً أيضاً على تكنولوجيا المعلومات ثانياً، بوصفها الداء والدواء لكل تلك المخاطر، وكذلك يبقى الأمل معقوداً على مستخدمي هذه التكنولوجيا، في رسم إشراقه غدٍ أفضل وخير أوفر، للإنسانية جميعاً.

هوامش الفصل الثاني:

١- ذياب البداينة: التحديات الأمنية في عصر العولمة، مجلة الدراسات الأمنية، ع١- عمان: أكاديمية الشرطة الملكية، ٢٠٠٤، ص ١٨-١٩.

٢- المرجع السابق نفسه . ص١٠-١١.

٣- المرجع السابق نفسه . ص ١٤.

٤- قسطنطين زريق. في معركة الحضارة . ط٣- بيروت: دار العلم للملايين، ١٩٧٧، ص ٣٧٧.

٥- المرجع السابق نفسه. ص ٣٧٧.

٦- جعفر حسن الطائي: صراع الحضارات وحقيقة المواجهة: جريدة الدعوة الإسلامية العالمية ع ٦٩٧.- طرابلس: جمعية الدعوة، ١٤٣٠ من وفاة الرسول ص ٩.

٧- مفيد الجوخدار: الحضارة والبيئة: مجلة المجلس العربي للاختصاصات الطبية، م٣، ع٢.- دمشق: المجلس العربي للاختصاصات الطبية، ٢٠٠١ ص ٨.

٨- السيد بخيت محمد. نقمة ثورة المعلومات . مجلة العربي، ع ٤٦٨- الكويت: وزارة الإعلام، ١٩٩٧. ص١٤٤.

٩- المرجع السابق نفسه . ص ١٤٤-١٤٥.

١٠- نبيل علي. العقل العربي وسط إعصار المعلومات : مجلة العربي، ع ٤٩٤- الكويت: وزارة الإعلام، ٢٠٠٠. ص٢٩.

١١- السيد بخيت محمد: مرجع سابق . ص ١٤٦.

١٢- عادل ريان: الحاسوب وأمراضه. في مستقبل الثورة الرقمية: العرب والتحدي القادم- الكويت: مجلة العربي، ٢٠٠٤. ص ١٥٨-١٥٩.

١٣- المرجع السابق نفسه ص ١٥٩-١٦١.

١٤- نبيل علي: الثقافة العربية وعرض المعلومات: رؤية لمستقبل الخطاب الثقافي العربي - الكويت: المجلس الوطني للثقافة والفنون والآداب. - (سلسلة عالم المعرفة؛ ٢٦٥)، ٢٠٠١، ص ١٣٩.

١٥- مي العبد الـلـه سنو: الاتصال في عصر العولمة: الدور والتحديات الجديـدة. - ط٢، منقحـة ومزيـدة- بـيروت: دار النهضة العربية ، ٢٠٠١. ص ٦٣-٦٤.

١٦- المرجع السابق نفسه: ص ٦٦-٦٧.

١٧- نبيل علي. الثقافة العربية وعصر المعلومات. مرجع سابق. ص ٤٢.

١٨- المرجع السابق نفسه: ص ٤٤-٤٥.

١٩- المرجع السابق نفسه: ص ٤٠٠-٤٠٢.

٢٠- المرجع السابق نفسه: ص٤٠٢.

٢١- عز الدين إسماعيل: تكنولوجيا الاتصال بين الفردية والجماعية: مجلة البحوث والدراسات العربية، ع٣٣- القاهرة: معهد البحوث والدراسات العربية، ٢٠٠٠، ص٥٠-٥٢.

٢٢- عـلي محمـد شـمو : الاتـصال الـدولي والتكنولوجيـا الحديثـة: الإنترنـت، القمـر الـصوتي الرقمـي، الملتميـديا- الإسكندرية: مكتبة ومطبعة الإشعاع الفنية، ٢٠٠٢، ص ٢٣٦.

٢٣- المرجع السابق نفسه: ص ٢٣٧-٢٣٩.

٢٤- عز الدين إسماعيل. المصدر السابق. ص ٥٤.

٢٥- شريـف درويـش اللبـان، أخلاقيـات المعلومـات في العـصر الإلكـتروني: رؤيـة مـستقبلية للجوانـب الأخلاقيـة للمعلومـات في الـوطن العـربي. مجلـة البحـوث والدراسـات العربيـة، ع ٣٣ - القـاهرة: معهـد البحـوث والدراسات العربية، ٢٠٠٠. ص ١٥٥.

٢٦- علي محمد شمو. المرجع السابق ص ٢٢٧.

٢٧- المرجع السابق نفسه. ص ٥٧-٦٠.

٢٨- شريف درويش اللبان: أخلاقيات المعلومات في العصر الإلكتروني/ رؤية مستقبلية. مرجع سابق . ص ١٤٣.

٢٩- المرجع السابق نفسه. ص ١٤٣.

٣٠- شريف كامل شاهين . الانترنت ومخاوفها. الرقابة مـسؤولية الفـرد أولاً وأخـيراً. مجلـة المكتبـات نـت، م١، ع ٩ (سبتمر)، ٢٠٠٠. حسن ١١-١٢.

٣١- المرجع السابق نفسه. ص ١٢-١٣.

٣٢- المرجع السابق نفسه. ص ١٣.

٣٣- عبد الرحمن بن عبد الله. الأمن والعولمة. مجلة الأمن والحياة، ع ١٩٣- الرياض: أكاديمية نايف العربية للعلوم الأمنية، ١٩٩٨. ص ٤٩.

٣٤- السيد يسين. ثورة المعلوماتية. في التقرير الاستراتيجي العربي - القاهرة: مركز الدراسات السياسية والإستراتيجية، ٢٠٠٠، ص ٣٨.

٣٥- فايز الشهري. الإعلام الإلكتروني والأمني. في ندوة الأمن والحياة. مجلة الأمن والحياة، ع ٢٣٢. الرياض: أكاديمية نايف للعلوم الأمنية، ٢٠٠١.ص ٢٥-٢٦.

٣٦- السيد يسين. مرجع سابق. ص ٣٨-٤٠.

٣٧- فايز الشهري. مرجع سابق. ص ٢٦-٢٧.

٣٨- السيد يسين. مرجع سابق. ص ٤٠-٤١.

٣٩- السيد علي شتا: الاغتراب في التنظيمات الاجتماعية - الاسكندرية: مكتبة الإشعاع، ١٩٩٧. ص ١٥٧-١٥٨.

٤٠- هشام محمد الحرك: المعلوماتية وامتلاك الغد.

http://www.rezgar.com/debat/show.art.asp.

العدد، ٥٨٢، ٢٠٠٣/٩/٥.

٤١- المرجع السابق نفسه.

٤٢- المرجع السابق نفسه.

٤٣- عمر عسوس. ووسائل الاتصال وتأثيرها على سلوك الأفراد. مجلة الأمن والحياة، ع ١٩٣. - الرياض: أكاديمية نايف العربية للعلوم الأمنية، ١٩٩٨. ص ٥٠.

٤٤- علي الباز، الإعلام والإعلام الأمني. (د.م) : مكتبة ومطبعة الإشعاع، ٢٠٠١، ص ١٠١.

٤٥- المرجع السابق نفسه. ص ١٠٢-١٠٣.

٤٦- عمر عسوس. مرجع سابق. ص ٥١.

٤٧- المرجع السابق نفسه. ص ٥١.

٤٨- علي الباز: مرجع سابق. ص ١٠٨-١١٥.

٤٩- ملفين. ل. ديظير وساندرا بول- روكيتشي: نظريات وسائل الاتصال. ترجمة كمال عبد الرؤوف - ط٣.- القاهرة: الدار الدولية للنشر والتوزيع، ١٩٩٩. ص ٦٠.

٥٠- عبد الرحمن محمد أبو توتة: علم الإجرام. بيروت: الجامعة المفتوحة، ١٩٩٤، ص ٢٠٧-٢٠٨.

الفصل الثالث




ظاهرة جرائم تكنولوجيا المعلومات
التعريف والتاريخ
والخصائص والتصنيف

تقديم

أضحت تكنولوجيا المعلومات تمثل سمة من سمات العصر الراهن، وبالتالي صار لزاماً على كل مجتمع يريد أن يتعايش، بل ويتواصل مع المجتمعات الأخرى، عليه أن لا يجهل أو يتجاهل أهميتها أو يعيش بدونها، أضف إلى ذلك، أن التطور الحاصل في عالم تكنولوجيا المعلومات بات يدعو إلى التوقف والتأمل إزاء هذه الظاهرة التكنولوجية، أكثر مما يدعو للدهشة. لقد باتت تكنولوجيا المعلومات الرئة الجديدة التي يتنفس منها أبناء مجتمع المعلومات العالي، لا بل أصبحت بمثابة القلب للجسم الإنساني وبقدر ما يمثل هذا التطور الحاصل في مجال تكنولوجيا المعلومات من إيجابيات، فإنه في ذات الآن، له العديد من السلبيات، وقد تكون في بعض الأحيان مهددة لسيادة الدولة، وفي البعض الآخر قد تكون قاتلة لعدد من أبناء هذه الدولة أو تلك.

منذ فترة زمنية ليست قصيرة، جعل العديد من الناس، بل والحال ينطبق على العديد من الدول، جعلوا حياتهم رهناً بأجهزة تكنولوجيا المعلومات، إذ أن قرارات الحروب أصبحت مرهونة أو محكومة بأزرار إلكترونية، بمجرد الضغط عليها تحل كارثة بالإنسانية. علاوة على ذلك، فإن الاقتصاد العالمي الحالي هو الآخر ينمو تحت وطأة الأزرار الإلكترونية.

نستنتج مما سبق، أن التقدم الحاصل في مجال تكنولوجيا المعلومات، فرده إلى التطور المتلاحق في برامج الكمبيوتر (Soft ware) أقل كما يرى المراقبون إذا تمت مقارنته بذلك الحاصل في عتاد الكمبيوتر (Hard ware) فتلك البرامج الموجودة الآن على الساحة التقنية، لا تعمل دائماً بكفاءة عالية، ولا يمكن الوثوق بها، وقد تؤدي لضياع الوقت والجهد والمال إذا أصابها خلل أو العطب فجأة. بيد أن الأمر الأخطر في ذلك، أنها قد تسبب في العديد من الكوارث التي تدعونا للتوقف أمامها كثيراً، قبل أن نفوض أمرنا لمثل هذه الأجهزة الإلكترونية المبرمجة.

١- ظاهرة جرائم تكنولوجيا المعلومات والتسميات المتعددة:

مما لا شك فيه ثمة تباين أو عدم ثبات حول المصطلحات والتسميات التي أطلقت، ولا زالت تطلق على هذه الظاهرة الإجرامية الجديدة التي باتت تهدد الدول قبل الأفراد، وربما مرد هذا التباين في المفاهيم، يعود إلى نشأة وتاريخ وتطور تكنولوجيا المعلومات أولاً، ومن ثم يعود إلى تطور وتمحور ظاهرة جرائم تكنولوجيا المعلومات ثانياً. واختلاف وجهات النظر بين المختصين في مجال الإعلام وبين رجال القانون وعلماء الاجتماع وعلم النفس ثالثاً.

لقد تعددت التسميات بشأن هذه الظاهرة الإجرامية، فمرة تسمى جرائم الكمبيوتر والإنترنت، ومـرة ثانيـة جـرائم التقنية العاليةن ومرة ثالثة الجريمة الإلكترونية، ومرة رابعة الاحتيال المعلوماتي، ومرة خامـسة احتيـال الحاسـوب، ومـرة سادسة غش الحاسوب، ومرة سابعة نصب الحاسوب، ومرة ثامنة الغش المعلوماتي أو الجريمة المعلوماتيـة، ومـرة تاسـعة جرائم الهاكرز، ومرة العاشرة الاختراقات التقنيـة، ومـا قيـل الأخـير الـسيبركرايم (cyber crime) وأخـيراً أصـحاب الياقـات البيضاء.

أمام هذا الواقع المتشظي من حيث تعدد التسميات المطلقة على هذه الظاهرة الإجراميـة الجديـدة عـلى المجتمـع الإنساني، لاسيما وأنها حدثت وسوف تحدث فقط في مجتمع المعلومات العالمي، أي المجتمع الـذي يـستخدم تكنولوجيـا المعلومات في معظم قطاعات الحياة فيه، لذلك يتطلب الأمر وضـع عنـوان جـامع شـامل تنـضوي تحتـه كـل التـسميات السابقة، وربما حتى التسميات اللاحقة إذا كانت تسميات جزئية. فـنحن بـدورنا أطلقنـا عليهـا تـسمية جديـدة نكـاد لم نلمسها في الأدبيات التي تناولت هذا الموضوع، تمثلت هذه التسمية بـ (جرائم تكنولوجيا المعلومات)[*].

تعد جرائم تكنولوجيا المعلومات ظاهرة إجرامية مستجدة نسبياً تقرع في جنباتها أجـراس الخطـر لتنبـه مجتمعـات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها، بوصفها تستهدف الاعتداء عـلى المعطيـات بـدلالتها التقنيـة الواسعة، (بيانات ومعلومات وبرامج بكافة أنواعها). فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمـون أذكيـاء يمتلكـون أدوات المعرفة التقنية، توجّه للنيْل من الحق في المعلومات، وتطال اعتداءاتها معطيـات الكمبيـوتر المخزنـة والمعلومـات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت. هذه المعطيات هي موضوع هـذه الجريمـة ومـا تـستهدفه اعتداءات الجنـاة، وهـذا وحـده - عـبر دلالتـه العامـة- يظهـر مـدى خطـورة جـرائم الكمبيـوتر، فهـي تطـال الحـق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي، والسيادة الوطنية، وتشيع فقدان الثقـة بالتقنيـة، وتهـدد إبداع العقل البشري. لذا فإن إدراك ماهية جرائم الكمبيوتر والإنترنت، والطبيعـة الموضـوعية لهـذه الجـرائم، واسـتظهار موضوعها، وخصائصها، ومخاطرها، وحجم الخسائر الناجم عنها، وسمات مرتكبيهـا، ودوافعهـم، يتخـذ أهميـة اسـتثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية الاجتماعية والثقافية. (١)

(*) المؤلف.

يمكن القول بشكل عام: إذا كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام، فإن خطر جرائم الكمبيوتر والإنترنت المحتمل في البيئة العربية يمكن أن يكون كبيراً باعتبار أن الجاهزية التقنية والتشريعية والأدائية (إستراتجيات حماية المعلومات) لمواجهتها ليست بالمستوى المطلوب إن لم تكن غائبة تماماً، وبالمقابل فقد أمست جرائم الكمبيوتر والإنترنت من أخطر الجرائم التي تقترف في الدول المتقدمة، لاسيما الأمريكية والأوروبية، ولهذا تزايدت خطط مكافحة هذه الجرائم وانصبت الجهود على دراستها المتعمقة وخلق آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية لاسيما المنظمات والهيئات الإقليمية الأوربية.

إن أكثر مسائل ظاهرة جرائم الإنترنت والكمبيوتر إثارة للجدل، إلى جانب تعريفها وتحديد موضوعها أو مناط الحماية ومحله، مسألة تحديد قائمة جرائم الكمبيوتر، وتحديد أنماط السلوك الإجرامي، والأفعال المكونة له.(٢)

٢- تعريف جرائم تكنولوجيا المعلومات:

قبل الخوض والخوض في تعريف جرائم تكنولوجيا المعلومات، لا بد من تعريف تكنولوجيا المعلومات بوصفها الأداة التي ترتكب عبرها أو من خلالها هذا النوع من الجرائم. وهناك تعريفات عديدة إلا أننا رأينا أن التعريف الذي وضعته اليونسكو هو الأكثر تماشياً هنا. إذ عرفتها منظمة اليونسكو بأنها (مجالات أو فروع المعرفة العلمية والتكنولوجية والهندسية والأساليب الإدارية المستخدمة في تناول ومعالجة المعلومات وتطبيقاتها. والمرتبطة بالحاسبات أو الحواسيب الآلية وتفاعلها مع الإنسان وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية)(٣).

أما بخصوص تعريف جرائم تكنولوجيا المعلومات، فمثلما تعددت التسميات التي أطلقت على هذا النوع من الجرائم، كذلك تعددت التعريفات في هذا المجال. بشكل عام يمكن القول: إن الإجرام المعلوماتي (هو ذلك الإجرام الذي يتم بطريق الحاسب الآلي والإنترنت - كذلك (هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي، والذي يميل فيه المجرم إلى العنف، ولذلك فالصورة التي نحن بصددها يطلق عليها الإتلاف المعلوماتي الناتج عن تقنيات تدمير ناعم.(٤) وتعرف جرائم تكنولوجيا المعلومات بأنها (كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات) (٥). وكذلك يمكن تعريف جريمة الحاسوب (بأنها الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة ومصلحة الأفراد خاصة)(٦).

أضف إلى ذلك، هناك من يعرف الجريمة المعلوماتية بأنها (تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي) (٧) ونلاحظ في هذا التعريف أنه يركز على الحاسب ويتجاهل دور الإنسان في تسخير الحاسب لتنفيذ ما يروم إليه. وتعرف أيضاً بأنها (كل جريمة ضد المال مرتبطة بالمعالجة الآلية للبيانات)(٨) اختصر التعريف على جريمة المال فقط وأهمل الجرائم الأخرى التي يمكن أن ترتكب عبر أو بواسطة أجهزة تكنولوجيا المعلومات علاوة على ذلك هناك تعريف يصف جرائم الإنترنت بأنها تمثل مجموعة الأفعال والأعمال غير القانونية التي تتم عبر شبكة الإنترنت أو تبث عبر محتوياتها. ويلاحظ أن شبكة المعلومات الدولية (الإنترنت) تمثل أحدث تكنولوجيا العصر التي تم استخدامها في مختلف جوانب الحياة ولكن البيانات والمعلومات تبين أن هناك أنماطاً من الجريمة تتم عبر الإنترنت، إلا أن هذا الوجه الإيجابي لهذه المخترعات (الإنترنت) يقابله وجه سلبي في ذات الوقت تمثل في استخداماتها سرقة المعلومات وبعض الأمراض والحشرات التي تهاجم الحاسبات وتصيبها بالتلف والأعطال، هذه الأعمال ينخرط فيها فنيون وذوو خبرة في عالم الحاسب محاولين بذلك إثبات ذاتهم ولو عن طريق تصميم برامج تهدد ذلك الإنجاز العلمي الضخم، وقد بدأت هذه الأفعال بانتهاكات فردية (سرقة برامج ، كتب، مستندات وملفات) ثم تطورت حتى أضحت ظاهرة عامة (تصميم الفيروسات لتصيب مكونات الشبكة، سرقة أسرار الصناعة التكنولوجية لأجهزة من شركة) الأمر الذي لفت الانتباه إلى أهمية تطبيق نظم الأمان برغم تكلفته الكبيرة.(٩)

أما في الوقت الحاضر فقد تبنى مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين تعريفاً جامعاً لجرائم الحاسب الآلي وشبكاته، حيث عرف الجريمة المعلوماتية بأنها (أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية)(١٠).

أمام تلك التعريفات المتعددة والصادرة عن وجهات نظر قانونية واجتماعية ونفسية وفلسفية أحياناً، يمكن بدورنا أن نضع لها تعريفاً آخر، يتمثل في ان جرائم تكنولوجيا المعلومات هي (كل فعل وعمل وكل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن إرادة جنائية يقوم به شخص ما له دراية ومعرفة بتكنولوجيا المعلومات المختلفة (تكنولوجيا التخزين والاسترجاع وتكنولوجيا الاتصالات الحديثة) ويوجه ضد المصلحة العامة والخاصة، وتشتمل تلك الجرائم من الناحية المبدئية جميع الجرائم التي يمكن أن ترتكب فيه أو عبر وسط إلكتروني، ويقرر لها القانون عقوبة أو تدبيراً).

٣- ظاهرة جرائم تكنولوجيا المعلومات : التاريخ والخسائر.

لقد حاول العديد من الباحثين في مجال القانون وعلم الاجتماع وعلم النفس بصورة عامة والمهتمين في مجال تكنولوجيا المعلومات بشكل خاص تقديم قبس الافصاح عن جرائم عالم تكنولوجيا المعلومات، وذلك من الكشف عن مخابىء المهام والأعمال الإجرامية التي يقوم بها مرتكبوا هذا النوع من الجرائم بيد أن عملية تدوين وتسجيل تلك العمليات الإجرامية، وما جرى في مستواها، لا زالت عبارة عن تسليط بقعة ضوء هنا وهناك لم تصل بعد إلى مستوى النضوج؛ وذلك بكل تأكيد إلى سببين أساسين هما:

١- السلوك الإجرامي وطبيعة العملية الإجرامية الإلكترونية وطبيعة الظروف والملابسات المحيطة بالجريمة.

٢- الخوف والتخوف من قبل الشركات والمؤسسات التي تتعرض إلى هذا النوع من الجرائم من التبليغ عن مثل هذه الجرائم لكي لا تخسر زبائنها.

لا ندعي هنا بأننا سوف نسجل أو نكتب التاريخ لكل جريمة من جرائم تكنولوجيا المعلومات بقدر ما تبقى محاولة لمتابعة تاريخ جرائم تكنولوجيا المعلومات، وربما هذه المحاولة عبارة عن مفاتيح للدخول إلى عالم ما زال مجهولاً للعديد من المتابعين والمهتمين بجرائم تكنولوجيا المعلومات. بيد أننا نظل معرضين لسلطة السؤال الباحث عن ميلاد جرائم تكنولوجيا المعلومات وعن زمن الكشف عنها. وللإجابة عن هذا السؤال والانفلات من سلطته رهينان باستدعاء التاريخ، حيث يتطلب الأمر الرحيل والوقوف بين ردهات الزمن للوقوف على البدايات الأولى لهذا العالم المرعب، والذي جعل العالم يعيش أو يتعايش مع نوع جديد من الجرائم لم تألفه الإنسانية من قبل.

إذا نظرنا إلى تاريخ الكمبيوتر والإنسان الآلي (الروبوت) نظرة متأنية لوجدناه حافلاً بارتكاب العديد من جرائم القتل التي لم تتم محاسبتهما حتى الآن! أضف إلى ذلك تسببا في الخسارات المادية التي لا حدود لها... الخ.

يقول الرجل الصفيحي في رائعة (أوزي) في عام (١٩٣٩): " أنا أغنّي، أنا أرقص، أنا ألعب دوري.. لو كان عندي قلب". وفي عام (١٩٥١) قال (لويس مومفورد): "احذر من المهندسين... إنهم يبدأون بماكينات الخياطة وينتهون بالقنبلة الذرية!". وفي الخامس من أكتوبر عام (١٩٦٠) كادت تنشب حرب عالمية ثالثة عندما حذر نظام الإنذار المبكر الصواريخ "الباليستية" في "جرينلاند"

البيت الأبيض من ان الولايات المتحدة تتعرض لهجوم هائل بالصواريخ السوفيتية آنذاك. واضطربت الدول الغربية ودول حلف شمال الأطلسي واستعدوا لإطلاق الصواريخ، كما انتظر الأمريكان قرار الكمبيوتر المركزي النهائي لبدء الهجوم، أكد الكمبيوتر أن البلاد تتعرض لهجوم بالصواريخ السوفيتية بنسبة يقين (٩٩.٩%!)، ولكن لم تبدأ الحرب عندما تم اكتشاف الحقيقة في آخر لحظة.(١١)

حدث في عام (١٩٦٠) نلمس جرائم تكنولوجيا المعلومات وبشكل واضح، إذ لوحظ زيادة مروعة في الجرائم بالكمبيوتر في البنوك الأمريكية، حيث قام موظفو البنك غير الأمناء باستبدال قسائم إيداع النقدية في حسابات العملاء بقسائم إيداع في حساب الموظف، وبذلك يتم إيداع النقدية في حسابه بدلاً من حساب العميل. وانتشر إتباع ذلك الأسلوب في الاختلاس حين بدأت البنوك في استخدام (ترميز الشيكات بالحبر الممغنط) (Magnetic ink character Recognition- MicR) ولم يكن هناك وقتها أساليب رقابية على هذا الاستخدام. ويقال إن أحد موظفي البنوك استطاع أن يختلس مبلغ (٢٥٠.٠٠٠) دولار في يوم واحد بإتباع هذا الأسلوب من الجرائم، وفي يوم ما صرف مبلغ (١٠٠٠.٠٠٠) دولار من حسابه الشخصي واختفى. (١٢).

من دراستين أجرينا في الولايات المتحدة عامي (١٩٨١-١٩٨٤) شملت أولاهما (٧٧) حالة احتيال بواسطة الحاسوب للاستيلاء على المال، وشملت الثانية (٦٧) حالة من نفس النوع، تبين أن (٥٢%) و (٤٢%) من مجموع حالات كل دراسة على التوالي قد اكتشفت عن طريق الرقابة الداخلية (Internal control) وأن (١٢%) و (٦%) من حالات كل منهما على التوالي اكتشفت عن طريق التدقيق الداخلي (Internal audit).(١٣)

في فبراير من عام (١٩٨٢) دخل عامل صياغة في مصنع "كاواساكي" في مدينة " أكسيكي" باليابان التاريخ من أبشع أبوابه. وأصبح "كينجي أوراداً أول إنسان يقتله الربوت، بعد أن حاول "كينجي" أن يفتح بوابة الأمان في "الروبوت" لقطع الطاقة عنه، ولكنه ضغط على زر التشغيل عن طريق الخطأ، فألقى الروبوت نظرة عليه، واعتبره أحد المكونات الصناعية، وأمسك بتلابيب الرجل وعصره، وقطعه إلى قطع صغيرة، وحوله في النهاية إلى "سجق"!.

في كارثة "تشير نوبيل" الشهيرة أخطأ الكمبيوتر في حساب بيانات نظام تبريد المفاعل، وهو ما أدى لحدوث الكارثة وتسرب الإشعاع. وفي مسح تم إجراؤه في المصانع الأمريكية التي تستعين بالرجل الآليين في العمل تبين أن نسبة لا تقل عن ٤% من الروبوتات العاملة في هذه المصانع تسببت

في حوادث عرضية قاتلة، مثل: تحطيم رؤوس المشغلين بالأسلحة القاتلة، أو تعليق عمال سيئي الحظ في الهواء، ونقلهم على حزام النقل، وطلائهم، وتحويلهم لأحد مكونات السيادات. وقد كانت أكثر الوفيات والإصابات نتيجة للحركة السريعة للأسلحة الآلية للآلات الذكية التي تسببت في سحق البشر، أو لصقهم في إحدى الماكينات الثقيلة دون أدنى شعور بالذنب!

تسبب الكمبيوتر في عام (١٩٨٣) في إحداث فيضان كبير على طول نهر "كولورادو" بالولايات المتحدة الأمريكية، وهو ما تسبب في حدوث أضرار بالغة وخسائر جسيمة تعدت قيمتها ملايين الدولارات واعترف حاكم "نيفادا بأن المتسبب في هذا الفيضان هو: " خطا ارتكبته الحاسبات الاتحادية". فقد قرر الكمبيوتر إهمال نسبة ذوبان الجليد في ربيع عام (١٩٨٣)؛ لأنه فضل التعامل بالمعدلات التي سجلها في السنوات السابقة بناء على قراره الشخصي الناتج عن التفكير "المنطقي"؛ ولذلك تدفقت كمية هائلة من الماء من فوق السدّ، وتسبب هذا الفيضان الناجم عن خطأ إلكتروني في موت ستة أشخاص.(١٤).

أضف إلى ذلك، أن جرائم تكنولوجيا المعلومات لم تتوقف عند هذا الحد، بل استمرت في الإزدياد، ففي دراسة مسحية لإدارة الصحة وخدمات الإنسان في الولايات المتحدة الأمريكية عام (١٩٨٣)، ظهر أن الحوادث العرضية والمصادقة (مثل الفضول أو الشكوى أو الانتقام من المبلغ ضده (الفاعل) أو الأنشطة غير العادية للجناة وتحديداً الانفاق غير العادي) كانت هي العامل المنبه لاكتشاف (٤٩%) من حالات غش الحاسوب، وأن التدقيق الداخلي والخارجي كان المنبه لاكتشاف (٢٩%)، بينما كانت الرقابة الشاملة (الرقابة الداخلية والتغيير غير المعتاد في مواعيد إجراء تقارير إدارة المحاسبة والرقابة على الانتهاكات الأمنية للحاسوب) المنبه لاكتشاف (٢٥%) من هذه الحالات.

كذلك حدث في ذات العام (١٩٨٣)، حاول مجموعة من الإرهابيين تفجير حاسب (شركة مان) الألمانية لاحتجاجهم على مساهمة الشركة في تطوير صواريخ حربية. وقد كانت الخسائر المالية كبيرة إلا أن ملفات البيانات الاحتياطية سلمت من الدمار. وفي اليابان، تم البلاغ عن (٢٨٨) جريمة متعلقة بأجهزة الصرف الإلكتروني في عام (١٩٨١)، ذلك الإبلاغ جاء في (١٩٨٣). وفي ذا العام، وفي كوريا الجنوبية، استطاع شاب بريطاني لا يتجاوز عمره السادسة عشرة التسلسل إلى قواعد بيانات تابعة لمركز أبحاث الطاقة النووية الكورية عبر شبكة الإنترنت التي ارتبطت بها شبكات المركز مؤخراً. ومن حاسب متواضع بمنزله في لندن استطاع طالب فاشل واسمه ريتشارد برايسن (١٦عاماً) أن يخترق شبكة معلومات القوات الجوية الأمريكية وهو في غرفة نومه.(١٥)

علاوة على ذلك ، فإن جرائم تكنولوجيا المعلومات ظلت آخذة بالازدياد، ففي دراسة أجريت عام (١٩٨٤) في كندا ونشرت نتائجها مجلة (الكمبيوتر والحماية) الأمريكية عام (١٩٨٤)، ظهر أن صافي معدل الخسارة الناجمة عن السطو المسلح (جريمة تقليدية) على البنوك (٣٢٠٠) دولار للحالة الواحدة وأن نسبة القبض على مرتكبيها تصل إلى (٩٥%)، بينما يصل معدل الخسارة الناجمة عن اختلاس أموال البنوك بدون استخدام الكمبيوتر حوالي (٢٣٥٠٠) دولار للحالة الواحدة، فإذا استخدم الحاسوب في ارتكاب الجريمة، فإن معدل الخسارة يرتفع بشكل حاد ليصل إلى (٤٣٠٠٠٠) دولار وتنخفض نسبة فرص ضبط الجناة من (٩٥%) إلى (٥%) أما فرص الضبط والملاحقة القضائية معاً فتنخفض إلى أقل من (١%). ومن منتصف الثمانينات ثمة حجم خسائر كبيرة تتكبدها كبرى شركات المال والبنوك والمؤسسات في الدول المتقدمة، الاقتصادية والعسكرية والعلمية، جراء جرائم الكمبيوتر، كإفشاء البيانات السرية المعالجة في نظم الحاسوب والاتجار بالمعلومات وتدمير نظم التشغيل وجرائم الفيروسات وقرصنة البرامج، وغيرها. والأمر الذي بات مؤكداً، أن جرائم الكمبيوتر أكثر خطورة من الجرائم التقليدية، تخلف حجماً كبيراً من الخسارة، وتشيع القلق وتهدد مستقبل سوق المال، وتمس حق الأفراد في المعلومات، إلى جانب خطرها على السيادة الوطنية.

فيما يخص الجانب التاريخي كذلك، وعلى صعيد التضرر الاقتصادي، تعد الولايات المتحدة الأمريكية، الدولة الأكثر تضرراً من جرائم الكمبيوتر، فإن التقرير الصادر عن وزارة العدل الأمريكية عام (١٩٨٦)، يشير إلى أن البنوك الأمريكية تكبدت خسائر جسيمة خلال السنوات الخمس السابقة لعام (١٩٨٦) من جراء (١٣٩) حالة من حالات الاحتيال والخطأ وقعت أثناء التعاملات التي أجريت عبر الوسائل الإلكترونية لتحويل الاعتمادات والأموال، وقد بلغ معدل الخسارة بالنسبة للحالة الواحدة (٨٣٣.٢٧٩) دولار، أما أقصى خسارة فقد بلغت (٣٧) مليون دولار، وفي (٦%) من الحالات المذكورة كان مرد الخسارة هو الاحتيال (غش الكمبيوتر) للاستيلاء على المال.

تظهر دراسة نشرت في المملكة المتحدة عام (١٩٨٦) شملت (١٩٥) حالة احتيال أو غش الحاسوب للاستيلاء على المال النتائج الآتية:

١- (١٥%) من هذه الحالات اكتشفت نتيجة يقظة ودقة الإدارة ومهارتها في الرقابة على الإجراءات الكتابية واستعمال أساليب الرقابة على التطبيقات (البرامج التطبيقية).

٢- (١٠%) منها اكتشف بناء على شكاوى قدمها المجني عليهم.

٣- (٧%) اكتشفت أثر إجراء تغييرات في الإدارة نتيجة برمجة التطبيقات لتلاءم أجهزة وأنظمة معلوماتية جديدة.

٤- (١٥%) منها اكتشف بمحض الصدفة.

٥- (١٥%) منها اكتشف نتيجة معلومات سرية للشرطة ولرب العمل الذي يعمل لديه الفاعل.

٦- (٣%) منها كان اكتشافها نتيجة شكوك وريب من جانب الإدارة أو الزملاء في مصدر الثراء المفاجئ للجناة وإنفاقهم الأموال ببذخ.(١٦)

بيد أن الفعل الإجرامي في مجال جرائم تكنولوجيا المعلومات ظل آخذ بالإزدياد، إذ أن هذه الظاهرة بدأت تزداد بمرور الأيام، حتى لو كان الفاعل إنسان آلي وليس من دم ولحم. حيث يبدو أن الرجال الآليين يتطورون، ويصبحون أذكى مما نعتقد بمرور الوقت، وأنهم يطورون وسائلهم دائماً ففي إبريل عام (١٩٨٦) فوجيء عامل خط تجميع سيارات في أحد المصانع بعطل مفاجئ أصاب أحد الروبوتات العاملة، فقرر الانتقام منه بضربه بمطرقة ثقيلة، وعندما هم العامل برفع المطرقة لتدمير صندوق التحكم الذاتي لاصقة الروبوت، فقام بتغيير اتجاهه بسرعة، وأمسك بتلابيب العامل ورفعه لأعلى، ثم قام بإلقائه لمسافة بعيدة خارج سياج الأمان، ثم قام الروبوت بإيقاف نفسه عن العمل بعد ذلك!.

أضف على ذلك، وكما تسبب الخطأ البشري ورداءة البرمجيات في كارثة "تشيرنوبيل"، فقد تسببت في انفجار المكوك الفضائي "تشالينجر" في عام (١٩٨٦)، وغيرها من الكوارث الأخرى، عندما أهمل العلماء أو أساؤوا فهم بيانات الكمبيوتر اللازمة للحفاظ على حياة البشر.

وفي مايو (١٩٨٧) كان الكمبيوتر الكندي "تراك – ٢٥" ، (herac -٢٥) يعالج مرضى السرطان عن طريق قصف الأورام بموجات العلاج المشعة، وفجأة قرر الكمبيوتر زيادة الجرعة إلى (١٠٠) مرة ضعف الجرعة الأصلية، وهو ما تسبب في قتل مريضين في الحال، وتُوفي عدد آخر بعد ذلك نتيجة لتعرضهم لجرعة تزيد (٢٥) مرة عن الجرعة القاتلة.

علاوة على ذلك وفي عام (٢٠٠٠) أسقط نظام دفاعي سوفيتي طائرة نقل ركاب كورية، وتسبب في قتل جميع ركابها، بعد أن دخلت الطائرة إلى المجال الجوي السوفيتي نتيجة لحدوث خطا في برمجيات الطيار الآلي، واعتبر الكمبيوتر الروسي أن الطائرة الكورية المدنية هدفاً

عسكرياً عدائياً، وأهمل الاتصالات اللاسلكية والقراءات الرادارية والصور التي تؤكد عكس ذلك تماماً. واضطر الروس لتفسير الأمر بأن الطائرة كانت في مهمة تجسس للتغطية على حقيقة أن برامجهم كانت بطيئة وغبية في التعامل مع الموقف ، وتسببت في قتل الأبرياء.

كذلك لم تكن الكمبيوترات والبرمجيات الأمريكية أذكى من مثيلاتها الروسية؛ فقد حفلت الحروب الأمريكية الأخيرة بالعديد من الأخطاء التي تسببت في موت ملايين الأبرياء. وقد حفل تاريخ العسكرية الأمريكية بأخطاء مفزعة، ومن أشهر هذه الأخطاء قيام المدمرة الأمريكية "فينسينز" بإسقاط طائرة مدنية إيرانية نتيجة لخطأ بنظام الكمبيوتر "أيجيس" الذي اعتبر أن الطائرة المدنية الإيرانية هي طائرة "إف-١٤" المقاتلة، وقام بتوجيه صاروخين فقاما بنسف الطائرة الإيرانية نسفاً كاملاً خلال ثوانٍ معدودة، وهو ما تسبب في مقتل (٢٩٠) شخصاً.(١٧)

في ضوء ما تقدم، يمكن القول: إن تاريخ جرائم تكنولوجيا المعلومات يبقى عالماً فيه من دهاليز الظلام ربما أكثر من مناطق النور، وكل شكوى تقدم من قبل المتضرر أو خاسر، هي بمثابة تسليط بقعة ضوء على ذلك الحدث، وفي ذات الآن هو تسجيل لتاريخ لجريمة من جرائم تكنولوجيا المعلومات سواء ارتكبت من قبل فرد من داخل حدود البلد أو من قبل فرد أو منظمة من خارج أسوار الوطن. ولهذا وذاك فإن ردهات التاريخ مليئة بأحداث إجرامية ربما سيكون الزمن كفيل بشكف النقاب عنها، أو ربما تبقى عالقة في كهوف ذاكرة البشر المتضررين، وربما الظروف والملابسات المحيطة بالجريمة تبقى غامضة بحيث لا تسمح بقيس الإفصاح عنها؛ ولهذا فإن التواريخ السابقة هي بمثابة تلميح لا تصريح.

٤- ظاهرة جرائم تكنولوجيا المعلومات والخسائر: أرقام وتواريخ.

إذا كانت الفقرة السابقة تتحدث عن تاريخ جرائم تكنولوجيا المعلومات، فإن هذه الفقرة تتطرق تحديداً إلى خسائر التي تخلفها هذه الجرائم، ولكنها (أي تلك الخسائر) مدونة أو مرتبطة بزمن أو تاريخ محدد وفقاً لعدد من الدراسات المسحية التي أجريت من قبل مؤسسات تعنى بشؤون وأمن المجتمعات. ففي هذا المجال أعلن معهد أمن المعلومات (computer security institute) نتائج تقرير عام (٢٠٠١) وهو التقرير السادس حول جرائم الكمبيوتر ودراسة أمن المعلومات المسحية، CSI/ FBI Computer Crime and Security survey ٢٠٠١، وهذه الدراسة يتم إجراؤها سنوياً من قبل المعهد بالتعاون مع مكتب التحقيقات الفدرالية في الولايات المتحدة الأمريكية، بغرض رفع مستوى الوعي لمسائل أمن المعلومات وتحديد واقعها.

لقد أجريت هذه الدراسة الشاملة بمشاركة (٥٣٨) مؤسسة أمريكية تضم وكالات حكومية وبنوك ومؤسسات مالية ومؤسسات صحية وجامعات، وأظهرت بوجه عام تنامي خطر جرائم الكمبيوتر وارتفاع حجم الخسائر الناجمة عنها بالرغم من زيادة الوعي بإلحاق المعلومات، فقد تبين أن (٨٥%) من المشاركين في الدارسة وتحديداً المؤسسات الحكومية الكبرى تحرت اختراقات الكمبيوتر خلال السنة السابقة، وأن (٦٤%) لحقت بهم خسائر مادية جراء هذه الاعتداءات، وأن (٣٥%) تمكن من حساب مقدار خسائره المادية التي بلغت تقريباً (٣٧٨) مليون دولار في حين كانت الخسائر لعام (٢٠٠٠) بحدود (٢٦٥) مليون دولار وأن معدل الخسارة السنوية للأعوام الثلاثة السابقة لعام (٢٠٠٠) بلغت (١٢٠) مليون دولار، وأن أخطر مصادر الخسارة المالية تمثلت بسرقة المعلومات المتعلقة بالأموال والممتلكات (حوالي ١٥١مليون) والاحتيال المالي (حوالي ٩٣ مليون). وأظهرت الدراسة أيضاً أن (٧٠%) من الاعتداءات حصلت من نقطة الاتصال الخارجي عبر الانترنت مقابل (٣٠%) حصلت من نقطة تتعلق بداخل النظام نفسه، في حين كانت نسبة الاختراق عبر اتصال الإنترنت (٥٩%) في عام (٢٠٠٠). في حين أن (٣٦٥) من المشاركين بالدراسة قد أبلغوا جهات القانون حول هذه الاختراقات بزيادة بنسبة (١١%) عن عام (٢٠٠٠)، حيث كانت نسبة المبلغين (٢٥%)، عام (٢٠٠٠) في حين كانت (١٦%) عام ١٩٩٦.

أما حول مصدر وطبيعة الاعتداءات فإن (٤٠%) من الاعتداءات تمت من خارج المؤسسات مقابل (٢٥%) في عام (٢٠٠٠)، وأن (٣٨%) من الاعتداءات تعلقت بهجمات انكار الخدمة مقابل (٢٧%) عام (٢٠٠٠) وأن نسبة الموظفين الذين ارتكبوا أفعال إساءة استخدام اشتراك الإنترنت لمنافع شخصية بلغت (٩١%)، تتوزع بين الاستخدام الخاطيء للبريد الإلكتروني وتنزيل مواد إباحية من الشبكة، في حين كانت هذه النسبة (٧٩%) في عام (٢٠٠٠)، وأن (٩٤%) من المشاركين تعرضوا لهجمات الفيروسات مقابل (٨٥%) عام (٢٠٠٠).

أما فيما يتعلق بالتجارة الإلكترونية، فإن (٩٧%) من المشاركين لديهم مواقع على الإنترنت، وأن (٤٧%) منهم يتعامل بالتجارة الإلكترونية، وأن (٢٣%) قد تعرضوا لدخول غير المصرح به أو إساءة الاستخدام وأن (٢٧%) لا يعرفون فيما إذا كانت مواقعهم قد تعرضت لمثل هذه الاعتداءات، وأن (٢١%) من الجهات المشاركة التي تعرضت إلى اعتداءات أبلغت عن (٢-٥) حوادث، وأن (٥٨%) أبلغ عن عشرة حوادث فأكثر، وأن (٩٠%) من الاعتداءات كانت اعتداءات حاقدة مقابل (٦٤%) عام (٢٠٠٠)، وأن (٧٨%) من الاعتداءات تتعلق بإنكار الخدمة مقابل (٦٠%) عام (٢٠٠٠) وأن

(١٣%) أبلغوا عن سرقة معلومات مقابل (٨%) عام (٢٠٠٠) وأن (٨%) أبلغوا عن احتيال مالي مقابل (٣%) عام (٢٠٠٠).

والجدولان رقم (١) ورقم (٢) يبينان مقدار الخسائر لفترت زمنية محددة وغير محددة، إلا أن اللافت للنظر في هذه الجدوال أن الأرقام الموجودة لا تحتاج إلى تعليق كثير، لأنها تقوم بشكل دقيق بتقديم قيس الإفصاح والتصريح لا التلميح عن مقدار الخسائر الناتجة عن ارتكاب جرائم تكنولوجيا المعلومات.

جدول ١: خسائر جرائم الكمبيوتر وفق الدراسة المتقدمة للأعوام من ٩٧ وحتى الربع الأول من ٢٠٠١(١٨).

مصدر الخسائر/ الجريمة ونوع الهجوم	١٩٩٧	١٩٩٨	١٩٩٩	٢٠٠٠	٢٠٠١
Theft of proprietary into. سرقة المعلومات المتعلقة بالملكية	٢٠.٠٤٨.٠٠٠	٣٣.٥٤٥.٠٠٠	٤٢.٤٩٦.٠٠٠	٦٦.٧٠٨.٠٠٠	١٥١.٢٣٠.١٠٠
Sabotage of data networksإتلاف أو تخريب معطيات الشبكات	٤.٢٨٥.٨٥٠	٢.١٤٢.٠٠٠	٤.٤٢١.٠٠٠	٢٧.١٤٨.٠٠٠	٥.١٨٣.١٠٠
Telecom eavesdroppingتضمنت الشبكات	١.١٨١.٠٠٠	٥٦٢.٠٠٠	٧٦٥.٠٠٠	٩٩١.٢٠٠	٨٨٦.٠٠٠
System Penetration by outsider اختراق النظام من الخارج	٢.٩١١.٧٠٠	١.٦٣٧.٠٠٠	٢.٨٨٥.٠٠٠	٧.٨٨٥.٠٠٠	١٩.٠٦٦.٦٦٠
Insider abuse of Net access إساءة الدخول للشبكة من داخل المنشأة	١.٠٠٦.٧٥٠	٣.٧٢٠.٠٠٠	٧.٥٧٦.٠٠٠	٢٧.٩٨٤.٠٠٠	٣٥.٠٠١.٦٥٠
Financial Fraud الاحتيال المالي	٢٤.٨٩٢.٠٠٠	١١.٢٣٩.٠٠٠	٣٩.٧٠٦.٠٠٠	٥٥.٩٩٦.٠٠٠	٩٢.٩٣٥.٥٠٠
Denial of Service إنكار الخدمة	N/a	٢.٧٨٧.٠٠٠	٣.٢٥٥.٠٠٠	٨.٢٤٧.٥٠٠	٤.٢٨٣.٦٠٠
Spoofing التلاعب والخداع بطريق سبوفنغ	٥١٢.٠٠٠	N/a	N/a	N/a	N/a
Virus الفايروسات	١٢.٤٩٨.١٥٠	٧.٨٧٤.٠٠٠	٥.٢٧٤.٠٠٠	٢٩.١٧١.٧٠٠	٤٥.٢٨٨.١٥٠
Unauthorized insider Access الدخول غير المصرح به من الداخل	٣.٩٩١.٦٠٥	٥٠.٥٦٥.٠٠٠	٣.٥٦٧.٠٠٠	٢٢.٥٥٤.٥٠٠	٦.٠٦٤.٠٠٠
Telecom Fraud احتيال الاتصال	٢٢.٦٦٠.٣٠٠	١٧.٢٥٦.٠٠٠	٧٧٣.٠٠٠	٤.٠٢٨.٠٠٠	٩.٠٤١.٠٠٠
Active Wiretapping استراق السمع- المادي-	N/a	٢٤٥.٠٠٠	٢٠.٠٠٠	٥.٠٠٠.٠٠٠	٠
Laptop Theft سرقة الكمبيوتر المحمول	٦.١٣٢.٢٠٠	٥.٢٥٠.٠٠٠	١٣.٠٣٨.٠٠٠	١٠.٤٠٤.٣٠٠	٨.٨٤٩.٠٠٠
المجموع	١٠٠.١١٩.٥٥	١٣٦.٨٢٢.٠٠	١٢٣.٧٩٩.٠٠	٢٦٥.٥٨٦.٢٤	٣٧٧.٨٢٨.٧٠٠

جدول (٢) يبين خسائر جرائم الكمبيوتر بشكل عام. (١٩)

رقم الحالة	ملخص الحالة	مقدار الخسائر (١٠٠٠دولار)	فترة التنفيذ (سنوات)	نوع المخطط	نوع التلاعب في الكمبيوتر	الحسابات المدينة بقيمة التلاعب	وظيفة مرتكبي الجريمة الرئيسي	عدد مرتكبيها داخل / خارج المؤسسة	وسيلة اكتشاف الجريمة
١	وضع المحاسب في أحد مجلات الأقسام مودين ومشتريات وأذون دفع وهمية	١٠٠ دولار	١.٣	إنفاق	إضافة عمليات غير مصرح بها	المخزون	محاسب	١/-	شكوك أحد موظفي البنك
٢	أعد المختص في شركة تأمين طلبات دفع تعريضات وهمية بأسماء أصدقاء ترتب عليها إصدار شيكات دفع التعويضات آليا بواسطة الكومبيوتر.	١٢٨ دولاراً	٤	سداد تعويضات وهمية	إضافة عمليات غير مصرح بها	المصروفات	موظف إعداد طلبات التعويض	٢٢/١	خطأ وقع فيه أحد مرتكبي الجريمة
٣	أدخل كاتب المستودعات بيانات خاطئة في نظام المخزون الإلكتروني بغرض إخفاء سرقات قطع الغيار، وإصدار البضائع من المخازن بدون إعداد فواتير.	٤٠٠٠ دولار	٦	المخزون والفواتير	تغيير مدخلات العمليات	المخزون	مشغل المحطات الفرعية	١٣/١	اكتشاف العجز في المخزون خلال الجرد الفعلي أثناء عملية المراجعة
٤	استخدام كاتب المستودعات محطة الكمبيوتر الفرعية في مكتبه للتلاعب في أرصدة المخزون لإخفاء السرقات.	٢٠٠ دولار	١.٥	المخزون	استخدام المحطات الفرعية لإدخال عمليات غير مصرح بها	لا شيء (تمييز مواقع سجلات المخزون)	موظف المستودعات	عدداً كبيرا	شكوك زوجة مدير المؤسسة

٥	قام المحاسب في شركة أعمال معدنية بتزوير كشوف المرتبات والأجور لسرقة أموال الشركة.	١٠٠ دولار	٣	الرواتب والأجور	غير معروف	المصروفات	محاسب	١/-	فحص قامت به مصلحة الضرائب
٦	سرقة أحد مدراء بنك ما في مدينة لندن أموالاً من حسابات العملاء بطيئة الحركة.	٢٩٠ دولار	٥	تحويل أرصدة حسابات العملاء	إدخال وتعديل عمليات غير مصرح بها	حسابات العملاء بالبنك (دائنون)	موظف في مركز الكمبيوتر	١/-	غير معروف
٧	أساء أحد موظفي بنك ما استخدام محطة الكومبيوتر الفرعية في مكتبه لتسوية التلاعب في حسابات العملاء على حساب بعضها البعض من خلال عدم إثبات بعض العمليات أو تغيير بعضها أو تحويل بعض الأرصدة بدون تصديق.	١٤٠٠ دولار	٣	تسوية التلاعب في أرصدة العملاء لتغطية سرقة النقدية	التغيير في العمليات وإضافة البعض وعدم إثبات البعض الآخر	حسابات العملاء بالبنك (دائنون)	المشرف على صرافي البنك	١/-	عمليات مقامرة اكتشفها رجال الأمن
٨	قام أحد المدراء في شركة صناعية بإعداد برنامج كمبيوتر استخدمه للسرقة.	١٠٠٠ دولار	٢	الإنفاق والغش في الفواتير	التغيير في العمليات وكذلك القيام بعمليات غير مصرح بها	المخزون والمصروفات	رئيس قسم إنتاج	١/١	شكوك أحد الزملاء العاملين في الشركة
٩	تعاون أحد الموظفين في شركة مرافق عامة مع شخص خارجي بإزالة رصيد حساب أحمد العملاء باستخدام رموز تصحيح أخطاء الكمبيوتر، وتسلم مقابل ذلك رشوة كبيرة من هذا العميل.	٢٥ دولار (أو أكثر)	٢	تحصيل حسابات العملاء	عمليات غير مصرح بها	المصروفات (قيود تسوية)	مندوب خدمة العملاء	١/٢	شكوك أحد موظفي البنك
١٠	قام موظف في أحد متاجر التجزئة بعمل مشتريات وأذون دفع وهمية لحساب شركة يمتلكها أحد أصدقائه.	١٢٠ دولار	٣	الإنفاق	عمليات غير مصرح بها	المخزون	كاتب حسابات	١/١	شكوك أحد الزملاء

١١	استخدمت إحدى عصابات الإجرام عدداً من المتخصصين بتشغيل أجهزة الكمبيوتر في بنكين مختلفين للقيام بعمليات احتيال من خلال سحب شيك على حساب بنك وإيداع قيمته في حساب البنك الآخر بغرض إخفاء الرقة من هذا البنك. بدون إثبات أي من عمليات الصرف أو الإيداع في السجلات (Check Kiting)	٩٠٠ دولار	٤	التلاعب في أرصدة حسابات البنك	تغيير في العمليات	(فرق التوقيت في إيداع وسحب النقدية)	نائب المدير العام لشؤون الكمبيوتر	٣/٢	تأخير موظف المراسلة من تسليم الشيكات في الوقت المحدد
١٢	قام أحد المحاسبين في منشأة تجارة جملة كبيرة بإنشاء حسابات موردين وهمية في نظام المعلومات المحاسبية الإلكترونية الذي يشرف عليه.	١٠٠٠ دولار	٤	الإنفاق	عمليات غير مصرح بها	المخزون	المراقب المالي	١/-	الاعتراف
١٣	قام أحد المدراء في شركة سمسرة أوراق مالية باختلاس أموال الشركة باستخدام نظم الكمبيوتر التي يشرف على إدارتها.	٢٧٧ دولار	٣	التلاعب في أرصدة حسابات	عمليات غير مصرح بها	حساب الإيرادات (إيرادات الفوائد)	نائب المدير العام لشؤون الكمبيوتر	١/-	غير معروف
١٤	قم أحد الشركاء المتضامنين في شركة سمسرة أوراق مالية بتحويل أرصدة الشركة من النقدية إلى حسابه الخاص	٨١ دولار	٣	التلاعب في أرصدة حسابات النقدية	عمليات غير مصرح بها	المصروفات (قيود التسوية)	شريك ومدير مركز الكمبيوتر	١/-	غير معروف
١٥	تلاعب أحد المدراء في دار نشر وتوزيع كبيرة في نظم الكمبيوتر بهدف زيادة قيمة المبيعات وعدم إثبات حسابات الدائنين بهدف تعظيم قيمة أرباح فرع المؤسسة الذي يشرف عليه، وبالتالي حصوله على ترقية إلى وظيفة أعلى وظيفة الحالية	١١.٥٠٠ دولار	فترة طويلة	تعظيم المبيعات وتخفيض المصروفات	تغيير في برامج وملفات الكمبيوتر	حسابات العملاء	مدير فرع	٥/-	غير معروف

وفق المعطيات السابقة، يتضح إن الإنترنت تمت بشكل مذهل خلال السنوات العشرة الأخيرة، فبعد أن كانت شبكة أكاديمية صغيرة أصبحت تضم الآن ملايين المستخدمين في كافة المدن حول العالم، وتحولت من مجرد شبكة بحث أكاديمي إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها، ولهذا لم يتم بناء الشبكة في المراحل الأولى على نحو يراعي تحديات أمن المعلومات، فالاهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة.

بيد أن النظرة هذه تغيرت تماماً في ١٩٨٨/١١/٢، ويرجع ذلك إلى حادثة (موريس) الشهيرة، فقد استطاع الشاب (موريس) أن ينشر فيروساً إلكترونياً عرف (بدودة WORM موريس) تمكن من مهاجمة آلاف الكمبيوتر، مستفيداً من ثغرات الأمن التي تعامل معها (موريس)، عندما وضع أوامر هذا البرنامج (الفيروس) الشرير، وقد تسبب بأضرار بالغة أبرزها وقف آلاف الأنظمة عن العمل وتعطيل وإنكار الخدمة، وهو ما أدى إلى لفت النظر إلى حاجة شبكة الإنترنت إلى توفير معايير من الأمن، وبدأ المستخدمون يفكرون ملياً في الثغرات ونقاط الضعف. وفي عام (١٩٩٥) نجح هجوم مخطط له عرف باسم (IP- SPOOFING) (وهو تكنيك جرى وصفه من قبل BELL LABS في عام (١٩٨٥) ونشرت تفاصيل حوله في عام ١٩٨٩)، هذا الهجوم أدى إلى وقف عمل الكمبيوترات الموثوقة أو الصحيحة على الخط وتشغيل كمبيوترات وهمية تظاهرت أنها الكمبيوترات الموثوقة. وقد بدأت العديد من الهجمات تظهر منذ ذلك التاريخ مستفيدة من نقاط الضعف في الأنظمة، فقد شهد عام (١٩٩٦) هجمات إنكار الحزمة (DENIAL-OF- SERVICE ATTACKS)، واحتلت واجهات الصحافة في ذلك العام عناوين رئيسة حول أخبار هذه الهجمات والخسائر الناجمة عنها، وهي الهجمات التي تستهدف تعطيل النظام عن العمل من خلال ضخ سيل من المعلومات والرسائل تؤدي إلى عدم قدرة النظام المستهدف على التعامل معها أو تجعله مشغولاً وغير قادر على التعامل مع الطلبات الصحيحة، وشاعت أيضاً الهجمات المعتمدة على الإنترنت نفسها لتعطيل مواقع الإنترنت، وقد تعرضت كل من وكالة المخابرات الأمريكية، ووزارة العدل الأمريكية، والدفاع الجوي الأمريكي، وناسا للفضاء، ومجموعة كبيرة من مواقع شركات التقنية والوسائط في أمريكا وأوربا، وكذلك عدد من المواقع الإسلامية لهجمات من هذا النوع.

هذه التغيرات في وسائل الهجوم وحجم الأضرار الناجمة عنها أظهر الحاجة إلى التفكير بخطط الأمن مع مطلع التسعينات للدفاع عن النظم ومواقع المعلومات، وبدأت تظهر مع بداية التسعينات وسيلة (الجدران النارية FIRE WALLS) كإحدى وسائل الأمن المعلوماتي، وهي عبارة عن بوابة للتحكم بنقاط الدخول ما بين الشبكة والمستخدمين، واعتمد استراتيجيات متباينة، كإستراتيجية السماح للكافة بالدخول إلى المواقع مع منع من لا تريد الشبكة إدخالهم، أو استراتيجية منع الكافة من الدخول والسماح فقط لمن تريد الشبكة إدخالهم، وقد تطورت وسائل الجدران النارية واستراتيجياتها بشكل مذهل.

وفقاً لمركز شكاوي احتيال الإنترنت (IFCC)، فإن احتيال الإنترنت يصنف إلى سبعة أنواع رئيسية: احتيال المزادات، واحتيال عدم التسليم المادي، احتيال الأسهم، احتيال بطاقات الإئتمان، سرقة وسائل التعريف، فرص الأعمال والخدمات الإحترافية أو المهنية، هذا الاحتيال تزايد على نحو ملحوظ. ووفقاً للتقرير السنوي الثاني الصادر عن مؤسسة (ERNST and YouNG) (وهي مؤسسة متخصصة في خدمات الأعمال والرقابة والاستشارات وتعد من المؤسسات القائدة في هذا الحقل برأس مال "٩" بليون وبعد موظفين يصل على "٣٠" ألف في "١٣٠" دولة في العالم) فقد شارك أربعة آلاف وثلاثمائة خبير تقني من "٣٥" دولة في الدراسة التي أجرتها في عام (١٩٩٨) بقصد وضع تصور دقيق حول أمن المعلومات والمخاطر في بيئة تقنية المعلومات، ووفقاً لهذه الدراسات المنشورة تفصيلاً على موقع WWW.EY.CO، فإن الوعي بمسائل أمن المعلومات قد نما وتزايد عن السنوات السابقة بشكل ملحوظ، إذ يتوفر لدى (٧٥%) من المشاركين في الدراسة مستوى ما من القدرة على حماية نظم المعلومات، مقابل نسبة (٤١%) لعام (١٩٩٧)، وأن (٧٥%) من هؤلاء قادرين على توفير الحماية و (٤%) واثقين بقدر أكبر على تحقيق ذلك و (٢٨) واثقين تماماً من هذه القدرات، وان (٨٣%) من المشاركين واثقين من مقدرتهم على مواجهة الاعتداءات الخارجية.

أما حول المخاطر التي تهدد مؤسسات الأعمال فقد أظهرت الدراسة ازدياد هذه المخاطر بالرغم من زيادة وسائل الأمن وزيادة الوعي، فمعظم المشاركين يعتقدون أن المخاطر إزدادت في القطاعات الصناعية والمواقع الحكومية وبين المتنافسين في السوق عما كانت عليه في العام السابق، وأن جزءاً من المخاطر نما بسبب اتساع التجارة الإلكترونية. وقد طلبت الدراسة من المشاركين تقسيم المخاطر المحددة فيها إلى مخاطر محتملة أو مخاطر أو تهديدات خطرة. فبالنسبة للاستخدام غير المصرح به فقد احتل المرتبة الأولى من المخاطر بنسبة (٧٩%)، وان (٢١%) من المشاركين اعتبروه تهديداً خطراً، أما عن أنشطة الموظفين المخولين فقد احتلت نسبة (٧٨%)، وقد اعتبرها (٧%)

تهديدات خطرة. أما حول مخاطر الشبكات تحديداً فقد صنف هجمات الهاكرز في قمة المخاطر وأظهرت الدراسة أن منطقة أفريقيا وشرق آسيا هي الأكثر تعرضاً للخطر.

إن تقارير الوسائل الإعلامية عن مخاطر تقنية المعلومات وتحديداً الإنترنت تتزايد يوماً بعد يوم، وتشير إلى تنامي هذه الظاهرة وتحديداً الاختراقات والاعتداءات في بيئة الإنترنت من قبل الهاكرز وبعض المنظمات الإجرامية الإعلامية ومن قبل الموظفين داخل المنشأة، فوفقاً لمركز الاستراتيجيات والدراسات العالمية الأمريكي، فإن الشرطة الفدرالية الأمريكية قدرت أن حجم الجرائم الإلكترونية يصل إلى (١٠) بليون سنوياً لكن (١٧%) فقط من الضحايا يبلغون عن هذه الجرائم لواحدة أو أكثر من جهات ملاحقة الجريمة. ووفقاً لتقرير حديث لمكتب المحاسبة في الولايات المتحدة الأمريكية، فإن عدد الحوادث التي تعامل معها فريق سيرت "CERT" (وهو فريق فدرالي للتدخل السريع بشأن الجريمة الإلكترونية) ازداد من (١٣٤٣) حادثاً عام (١٩٩٣) إلى (٩٨٥٩) حادثاً في عام ١٩٩٩.

أما أهم الأحداث الشهيرة في هذا الحقل فهي عديدة، لكننا نكتفي في هذا المقام بإيراد أبرز الحوادث التي حصلت خلال السنوات الماضية بحيث نعرض لحوادث قديمة نسبياً وحديثة كأمثلة على تنامي خطر هذه الجرائم وتحديداً في بيئة الإنترنت، كما سنورد أمثلة من خلاصات تقارير المحاكم حول بعض الوقائع الشهيرة مع الإشارة إلى مواقع نشرها على شبكة الإنترنت.

١- قضية مورس: هذه الحادثة هي إحدى أولى الهجمات الكبيرة والخطرة في بيئة الشبكات، ففي تشرين الثاني عام (١٩٨٨) تمكن طالب يبلغ من العمر (٢٣) عاماً ويدعى (ROBERMORRIS) من إطلاق فايروس عرف باسم (دودة مورس) عبر الإنترنت، أدى إلى إصابة (٦ آلاف) جهاز يرتبط معها حوالي (٦٠٠٠٠) نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لا عادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على مورس بالسجن لمدة (٣) أعوام وعشر آلاف دولار غرامة.

٢- قضية الجحيم العالمي: تعامل مكتب التحقيقات الفدرالية مع قضية اطلق عليها اسم مجموعة الجحيم العالمي "GLOBAL HELL")، فقد تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض والشركة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية

الأمريكية، وقد أدين أثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة، وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلى مجرد الاختراق أكثر من التدمير أو النقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة.

٣- فايروس ميلسا: وفي حداثة هامة أخرى، انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول في تحقيق واسع حول إطلاق فايروس شرير عبر الإنترنت عرف باسم فايروس "MELISSA"، حيث تم التمكن من اعتقال مبرمج كمبيوتر من ولاية نيوجرسي في شهر نيسان عام (١٩٩٩) واتهم باختراق اتصالات عامة والتآمر لسرقة خدمات الكمبيوتر، وتصل العقوبات في الاتهامات الموجهة له إلى السجن لمدة (٤٠) عاماً والغرامة التي تقدر بحوالي (٥٠٠) ألف دولار، وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها (١٩) مذكرة.

٤- حادثة المواقع الإستراتيجية: وفي ١٩ تشرين الثاني (١٩٩٩) تم إدانة "Eric burns" من قبل محكمة فيرجينيا الغربية بالحبس لمدة (١٥) شهراً والبقاء تحت المراقبة السلوكية لمدة (٣) سنوات بعد أن أقر بذنبه وأنه قام وبشكل متعمد باختراق كمبيوترات محمية الحق فيها ضرراً بالغاً في كل من ولايات فيرجينيا واشنطن وإضافة إلى لندن في بريطانيا، وقد تضمن هجومه الإعتداء على مواقع لحلف الأطلسي إضافة على الإعتداء على موقع نائب رئيس الولايات المتحدة، كما اعترف بأنه قد أطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الأبيض، وقد قام (eric) بتصميم برنامج أطلق عليه (web bandit) ليقوم بعملية تحديد الكمبيوترات المترابطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها، وباستخدام هذا البرنامج اكتشف أن الخادم الموجود في فيرجينيا والذي يستضيف مواقع حكومية واستراتيجية منها موقع نائب الرئيس يتوفر فيه نقاط ضعف تمكن من الإختراق، فقام في الفترة ما بين آب (١٩٩٨) وحتى كانون الثاني (١٩٩٩) باختراق هذا النظام (٤) مرات، وأثر نشاطه على العديد من المواقع الحكومية التي تعتمد على نظام وموقع (USIA) للمعلومات، وفي إحدى المرات تمكن من جعل آلاف الصفحات من المعلومات غير متوفرة مما أدى إلى إغلاق هذا الموقع لثمانية أيام، كما قام بالهجوم على مواقع لثمانين مؤسسة أعمال يستضيفها خادم شبكة (LASER. NET) في

منطقة فيرجينيا والعديد من مؤسسات الأعمال في واشنطن إضافة على جامعة واشنطن والمجلس الأعلى للتعليم في فيرجينيا رتشموند ومزود خدمات إنترنت في لندن، وكان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت اسم (ZYKLON) أو باسم المرأة التي يحبها تحت اسم (CRYSTAL).

٥- الأصدقاء الأعداء: وفي حادثة أخرى تمكن أحد الهاكرز (الإسرائيليين) من اختراق أنظمة معلومات حساسة في كل من الولايات المتحدة الأمريكية والكيان الصهيوني، فقد تمكن أحد المبرمجين الإسرائيليين في مطلع عام (١٩٩٨) من اختراق عشرات النظم لمؤسسات عسكرية ومدنية وتجارية في الولايات المتحدة وإسرائيل، وتم متابعة نشاطه من قبل عدد من المحققين في الولايات المتحدة الأمريكية حيث أظهرت التحقيقات أن مصدر الاختراقات هي كمبيوتر موجود في الكيان الصهيوني فانتقل المحققون إلى الكيان الصهيوني وتعاونت معهم جهات تحقيق إسرائيلية، حيث تم التوصل للفاعل وضبطت كافة الأجهزة المستخدمة في عملية الاختراق، وبالرغم من أن المحققين أكدوا أن المخترق لم يتوصل إلى معلومات حساسة إلا أن وسائل الإعلام الأمريكية حملت أيضاً أخباراً عن أن هذا الشخص كان في الأساس يقوم بهذه الأنشطة بوصفه عميلا (لإسرائيل) ضد الولايات المتحدة الأمريكية.

٦- حادثة شركة أوميغا: مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة (omega) من مدينة (Delaware) ويدعى (Timothy Allen Lioyd) (٣٥ عاماً) تم اعتقاله في (١٩٩٨/٢/١٧) بسبب إطلاقه قنبلة إلكترونية في عام (١٩٩٦) (bomb) بعد (٢٠) يوماً من فصله من العمل استطاعت أن تلغي كافة التصاميم وبرامج الإنتاج لأحد كبرى مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم تحكم مستخدمة في (nasa) والبحرية الأمريكية، ملحقاً خسائر بلغت (١٠) مليون دولار وتعتبر هذه الحادثة مثالاً حياً على مخاطر جرائم التخريب في بيئة الكمبيوتر، بل اعتبرت أنها أكثر جرائم تخريب الكمبيوتر خطورة منذ هذه الظاهرة.

في ضوء ما تقدم ، إننا سنقف في أكثر من نقطة مهمة في هذه الدراسة، على المعالم الرئيسية لخطورة هـذه الجـرائم وحجم الخسائر الناجمة عنها عند تعرضنا لأنماطها وفئاتها والتمثيل على ذلك من واقع القضاء المقـارن، فإننـا نكتفـي في هذا المقام بإيراد أبرز مخاطرها عموماً، إضافة لما ذكرناه في فقرات في الفصل السابق، من هذه المخاطر الآتي:

١- تهدد جرائم الحاسوب عموماً الحق في المعلومات انسيابها وتدفقها واسـتخدامها، وهـذا الحـق، وإن يكـن محـل نقاش مستفيض في إطار حقـوق الجيـل الثالـث المؤسـسة عـلى التـضامن، فـإن الأهميـة الإسـتراتيجية والثقافيـة والاقتصادية للمعلومات، تجعل من أنماط الاعتداء عليها خطورة جدّ بالغة بكونها تهدد في الحقيقة البناء الثقافي والاقتصادي للدولة، وأثر ذلك الواسع عـلى التنميـة التـي اعـترف بهـا كحـق مقـرر للمجتمعـات تجـب حمايتـه ورعايته لكسر الهوة بين المجتمعات الفقيرة والغنية.

٢- إن بعض جرائم الحاسوب تمس الحياة الخاصة أو ما يسمى بحق الإنسان في الخصوصية، وهذه الجـرائم تخلـف وراءها إلى جانب الضرر الكبير بالشخص المستهدف في الاعتداء - شعوراً عريضاً لدى الأفراد بمخاطر التقنية، مـن شأنه أن يؤثر سلباً في تفاعل الإنسان مع التقنية، هذا التفاعل اللازم لمواجهة تحديات العصر الرقمي.

٣- تطال بعض جرائم الكمبيوتر الأمن القومي والسيادة الوطنية في إطار ما يعـرف بحـروب المعلومـات أو الأخـلاق في عصر التقنية، وتحديداً جرائم التجسس وجرائم الإستيلاء على المعلومات المنقولة خارج الحدود.

٤- تشيع جرائم الكمبيوتر والإنترنت فقدان الثقة بالتقنية، ليس لدى الأفراد فحسب، وإنما لـدى أصـحاب القـرار في الدولة، وهو ما سيؤثر في الحقيقة على استخدام التقنية في غير قطاع من قطاعات المجتمع، إن جرائم الكمبيـوتر وليدة التقنية تهدد التقنية ذاتها، وبالتالي تهدد الفجر المشرق للمستقبل، المؤسس على التفاعل الإيجـابي مـا بـين الإنسان والتقنية العالية.

٥- إن خطر جرائم الكمبيوتر والإنترنت أو بعضها على نحو أدق لا يمس التقنية ذاتها في درجة شيوع الثقة بها سواء لدى الأفراد أو الدولة فحسب ، بل تهدد أي الجرائم، مستقبل صناعة التقنية وتطورها، وهذا يتحقـق في الواقـع من ثلاث فئات من جرائم الكمبيوتر والإنترنت، جرائم قرصنة البرمجيات، وجـرائم التجـسس الـصناعي، وجـرائم احتيال الإنترنت المالي(٢٠).

٥- ما تقسيمات جرائم تكنولوجيا المعلومات؟

تقسم جرائم تكنولوجيا المعلومات وفقاً للدور الذي تلعبه في ميدان ارتكاب الجريمة، وتبعاً لذلك تقسم إلى ثمان مجموعات، وهي كالآتي:

١- المجموعة الأولى: تشمل الجرائم التي تتمثل في اختراق الحاسوب لتدمير البرامج والبيانات الموجودة في الملفات المخزونة بالحاسوب، وهذه هي من أخطر أنواع الجرائم، وهنا يقوم شخص متخصص بوضع أمر معين (command) لبرامج الحاسوب، وعند تنفيذ هذا الأمر يتم مسح كلي أو جزئي للملفات المرتبطة بهذه البرامج ويتم هذا النوع من الجرائم متعمدة.

٢- المجموعة الثانية: وتتمثل في الجرائم التي يتم بها استغلال البيانات المخزنة على الحاسوب بشكل غير قانوني، ومن أمثلتها الدخول إلى شبكة الحاسوب التي تحمل أرقاماً سرية محددة من خلال استخدام الحاسوب للحصول على مبالغ نقدية تحت هذا الرقم أو الاختراق لكشف الأسرار أو لأغراض أخرى.

٣- المجموعة الثالثة: تشمل الجرائم التي تتم باستخدام الحاسوب لارتكاب جريمة معينة أو التخطيط لها.

٤- المجموعة الرابعة: وتشمل الجرائم التي يتم استخدام الحاسوب بشكل غير قانوني من قبل الأفراد المخصص لهم باستخدامه. ومن أمثلة ذلك استخدام الموظفين أو العاملين بمركز الحاسوب للأجهزة بعد أوقات العمل الرسمية أو أثناءه مثل استخدامه في التسلية ببرامج الألعاب أو بعض الأغراض الشخصية غير المرتبطة بالعمل الرسمي أو الاستخدام العشوائي لمفاتيح الأوامر من الذين لا يجيدون استخدام الحاسوب.

٥- المجموعة الخامسة: وتتمثل في فيروسات الكمبيوتر، والفيروس ما هو إلا برنامج آخر موجود على الكمبيوتر يهدف إلى إصابة الكمبيوتر لإتلاف البرنامج وربما كان السبب في ازدياد الرعب من الفيروس هو التزايد الهائل في حجم الاعتماد على أجهزة الكمبيوتر وشبكاتها والخدمات العامة التي توفرها مراكز الحاسوب بالمصالح العامة والخاصة ودائماً ينتقل الفيروس عند استخدام وسيط تخزيني ملوث بفيروس من الفيروسات (Storage media) وعند إدخال الوسيط وتحميل البيانات (Loading Data) على الحاسوب يتم تدمير البيانات أو تعطيل استخدام البرامج الأصلية المخزنة على الحاسوب، وقد يتصادف إرسال مجموعة اسطوانات من جهة بالبريد ويكتشف بأن تكون ملوثة بفيروس لذا يفضل

تجربة هذه البيانات قبل تخزينها على الحاسوب الرئيسي وبعض الفيروسات موجود أصلاً بالجهاز ولكن تنشط من وقت لآخر عند تنفيذ بعض الأوامر أو الألعاب(٢١).

٦- المجموعة السادسة: عندما يكون الكمبيوتر هدفاً للجريمة (Target of an offense) وذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفايروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وكما في حالة الإستيلاء على البيانات المخزنة أو المنقولة عبر النظم. ومن أوضح المظاهر لاعتبار الكمبيوتر هدفاً للجريمة في حقل التصرفات غير القانونية، عندما تكون السرية (CONFDENTIALITY) والتكاملية أي السلامة (INTEGRITY) والقدرة أو التوفر هي التي يتم الاعتداء عليها، بمعنى أن توجه هجمات الكمبيوتر إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى والتكاملية، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون تخويل ودون أن يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر) وغالبية هذه الأفعال الإجرامية تتضمن ابتداء الدخول غير المصرح به إلى نظام الهدف والتي توصف بشكل شائع في هذه الأيام بأنشطة الهاكرز كناية عن فعل الاختراق.

تتخذ الأفعال التي تتضمن سرقة المعلومات أشكال عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء، وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء، فالكمبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها، وهذه تمثل هدفاً للعديد من الجهات بما فيها أيضاً جهات التحقيق الجنائي والمنظمات الإرهابية وجهات المخابرات والأجهزة الأمنية وغيرها، ولا يتوقف نشاط الاختراق على الملفات والأنظمة .

غير الحكومية، بل يمتد إلى الأنظمة الخاصة التي تتضمن بيانات قيّمة، فعلى سبيل المثال قد يتول أحد المخترقين للدخول إلى نظام الحجز في أحد الفنادق لسرقة أرقام بطاقات الائتمان. وتتضمن بعض طوائف هذا النمط أي الكمبيوتر كهدف أنشطة سرقة والاعتداء على الملكية الفكرية كسرقة الأسرار التجارية وإعادة إنتاج ونسخ المصنفات المحمية وتحديداً برامج الحاسوب، وفي حالات أخرى فإن أفعال الاختراق التي تستهدف أنظمة المعلومات الخاصة تستهدف

منافع تجارية أو إرضاء أطماع شخصية كما أن الهدف في هذه الطائفة يتضمن أنظمة سجلات طبية وأنظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها.

٧- المجموعة السابعة: عندما تجعل الكمبيوتر أداة الجريمة لارتكاب جرائم تقليدية: Atool in the commission of traditional offense.

كما في حالة استغلال الكمبيوتر للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في الإستيلاء على أرقام بطاقات إئتمان وإعادة استخدامها والإستيلاء على الأموال بواسطة ذلك، حتى أن الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها أو تحوير عمل الأجهزة الطبية والمخبرية عبر التلاعب ببرمجياتها، أو كما في إتباع الوسائل الإلكترونية للتأثير على عمل برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها وقتل ركابها.

٨- المجموعة الثامنة: عندما يكون الكمبيوتر بيئة للجريمة: وذلك كما في تخزين البرامج المقرضة فيه أو في حالة استخدامه لنشر المواد غير القانونية أو استخدامه أداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها. وطبعاً يمكن للكمبيوتر أن يلعب أكثر من دور في ذات الآن، ومثال ذلك أن يستخدم أحد مخترقي الكمبيوتر (هاكرز) جهازه للتوصل دون تصريح إلى نظام مزود خدمات إنترنت (مثل نظام شركة أمريكا أون لاين) ومن ثم يستخدم الدخول غير القانوني لتوزيع برنامج مخزن في نظامه (أي نظام المخترق) فهو قد ارتكب فعلاً موجهاً نحو الكمبيوتر بوصفه هدفاً (الدخول غير المصرح به) ثم استخدم الكمبيوتر لنشاط جرمي تقليدي (عرض وتوزيع المصنفات المقرصنة) واستخدم كمبيوتره كبيئة أو مخزن عندما قام بتوزيع برنامج مخزن في نظامه.(٢٢)

٩- المجموعة التاسعة: وتعد هي المجموعة الأكبر من بين الأفراد الذين يخترقون نظم الحاسبات الآلية فقط لممارسة الهواية ومعرفة مدى مقدرتهم على إنجاز ذلك وليس بهدف السرقة أو تدمير البيانات.(٢٣)

٦- ما أسس وأنواع تصانيف جرائم تكنولوجيا المعلومات؟

ثمة اتفاق على أن جرائم تكنولوجيا المعلومات ليست فئة واحدة أو نوعاً واحداً، وطالما أنه كذلك، فإن الأسس والتصانيف هي الأخرى لم تأت ضمن نوع واحد ، وإنما اختلفت باختلاف أنواع جرائم تكنولوجيا المعلومات، وكذلك فإن الاختلاف هذا مرده إلى وجهات النظر المختلفة والصادرة من قبل رجال وفقهاء القانون، وعلماء الاجتماع، وعلماء النفس وغيرهم من المهتمين بأمن وشؤون المجتمعات أينما كانوا. ولهذا يصنف الفقهاء والدارسون جرائم الحاسوب ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا يتعدد الحق المعتدى عليه فتوزع جرائم الحاسوب وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة.

بيد أن من الملاحظ أن هذه التقسيمات أو بعضها، لم تراع بعض أو كل خصائص هذه الجرائم وموضوعها، والحق المعتدى عليه لدى وضعها لأساس أو معيار التقسيم ، ورغم ذلك كان لا بد من استعراض كل انواع التصانيف من أجل معرفة كل الرؤى والتصورات لمفهوم الجريمة الحديثة وفق كل المعطيات المختلفة والمتعلقة بجرائم تكنولوجيا المعلومات.

أما أهم أنواع تصنيف جرائم تكنولوجيا المعلومات فهي:

أولاً: تصنيف الجرائم تبعاً لنوع المعطيات ومحل الجريمة:

إن التصنيف هو الذي ترافق مع موجات التشريع في ميدان قانون تقنية المعلومات، وهو التصنيف الذي يعكس أيضاً التطور التاريخي لظاهرة جرائم الكمبيوتر والإنترنت، ولهذا نجد أن جرائم الحاسوب بالاستناد إلى هذا المعيار يمكن تقسيمها ضمن الطوائف الآتية:

١- الجرائم الماسة بقيمة معطيات الحاسوب : وتشمل هذه الطائفة فئتين، أولهما، الجرائم الواقعة على ذات المعطيات ، كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية. وثانيهما، الجرائم الواقعة على ما تمثله المعطيات آلياً، من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف

الحصول على المال أو جرائم الاتجار بالمعطيات، وجرائم التحوير والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة آلياً واستخدامها).

٢- الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة: وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.

٣- الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات٩ التي تشمل نسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص والاعتداء على العلامة التجارية وبراءة الاختراع.

عندما نمعّن النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق ، إذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء إنصب على قيمتها أو ما تمثله. والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي)، لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.

أما من جهة أخرى، نجد أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج، وحماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات بالنظر لقيمتها أو ما تمثله والذي عرف بحماية (الأموال)، كل في ميدان وموقع مستقل، وهو في الحقيقة تمييز - ليس مطلقاً- بين حماية قيمة المعطيات، وأمنها، وحقوق الملكية الفكرية. ولا بد لنا من الإشارة، إن حماية أمن المعطيات.

(الطائفة الثانية): انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الطائفة الأولى الماسة بقيمة المعطيات بالنظر إلى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو اغشاء هذه المعلومات غالباً ما كان الحصول على المال مما يعد من الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم.

ثانياً: تصنيف الجرائم تبعاً لدور الكمبيوتر في الجريمة:

تم فيما تقدم شرح لدور الكمبيوتر في الجريمة، فقد يكون بهدف الاعتداء، بمعنى أن يستهدف الفعل المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر والشبكات، وهذا ما يعبر عنه بالمفهوم الضيق (لجرائم الكمبيوتر)، وقد يكون الكمبيوتر وسيلة ارتكاب جريمة أخرى في إطار مفهوم (الجرائم المرتبطة بالكمبيوتر)، وقد يكون الكمبيوتر أخيراً بيئة الجريمة أو وسطها أو مخزناً للمادة الجرمية، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن الدور الأول. جرائم التخزين، ويقصد بها تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها، والثاني: جرائم المحتوى أو ما يعبّر عنه بالمحتوى غير المشروع أو غير القانوني والاصطلاح الأخير استخدم في ضوء تطور أشكال الجريمة مع استخدام الإنترنت، وأصبح المحتوى غير القانوني، يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الإلكتروني للأموال وغيرها، باعتبار أن مواقع الإنترنت تتصل بشكل رئيس بهذه الأنشطة، والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي نفس الوقت كوسيلة لارتكابها.

وهذا التقسيم شائع بجزء منه (وهو تقسيم الجرائم إلى جرائم هدف ووسيلة) لدى الفقه المصري والفرنسي، وتبعاً له تنقسم جرائم الكمبيوتر إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات وإتلافها، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر، أما تقسيمها كجرائم هدف ووسيلة ومحتوى فإنه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في أوربا تحديداً، وأفضل ما يمكن هذا التقسيم الاتفاقية الأوروبية لجرائم الكمبيوتر والإنترنت لعام (٢٠٠١)، ذلك أن العمل منذ مطلع عام (٢٠٠٠) يتجه إلى وضع إطار عام لتصنيف جرائم الكمبيوتر والإنترنت وعلى الأقل وضع قائمة الحد الأدنى محل التعاون الدولي في مكافحة هذه الجرائم، وهو جهد تقوده دول أوروبا، لكن وبنفس الوقت بتدخل ومساهمة من قبل استراليا وكندا وأمريكا، وضمن هذا المفهوم نجد الاتفاقية المشار إليها تقسم جرائم الكمبيوتر والإنترنت إلى الطوائف الآتية - مع ملاحظة أنها تخرج من بينها طائفة جرائم الخصوصية لوجود اتفاقية أوروبية مستقلة تعالج حماية البيانات الاسمية من مخاطر المعالجة الآلية للبيانات، اتفاقية عام (١٩٨١).

لقد أوجد مشروع الاتفاقية الأوروبية تقسيماً جديداً نسبياً، فقد تضمن أربع طوائف رئيسة لجرائم الكمبيوتر والإنترنت:

١- الجرائم التي تستهدف عناصر (السرية والسلامة وموفورية)المعطيات والنظم وتضم:

أ- الدخول غير القانوني (غير المصرح به).

ب- الاعتراض غير القانوني.

ج- تدمير المعطيات.

د- اعتراض النظم.

ه- إساءة استخدام الأجهزة.

٢- الجرائم المرتبطة بالكمبيوتر وتضم:

أ- التزوير المرتبط بالكمبيوتر.

ب- الاحتيال المرتبط بالكمبيوتر.

٣- الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.

٤- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة – قرصنة البرمجيات-.

ثالثاً: تصنيف الجرائم تبعاً لمساسها بالأشخاص والأموال:

نجد هذا التصنيف شائعاً في الدراسات والأبحاث الأمريكية مع فروق بينها من حيث مشتملات التقسيم ومدى انضباطيته، كما نجده المعيار المعتمد لتقسيم جرائم الكمبيوتر والإنترنت في مشروعات القوانين النموذجية التي وضعت من جهات بحثية بقصد محاولة إيجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع، وهنا نعرض التقسيم الذي تضمنه مشروع القانون النموذجي لجرائم الكمبيوتر والإنترنت الموضوع عام (١٩٩٨) من قبل فريق بحثي أكاديمي، والمسمى (Model state computer crimes cod)، وفي نطاقه تم تقسيم جرائم الكمبيوتر والإنترنت إلى الجرائم الواقعة على الأشخاص، والجرائم الواقعة على الأموال عدا السرقة، وجرائم السرقة والاحتيال، وجرائم التزوير، وجرائم المقامرة والجرائم ضد الآداب- عدا الجرائم الجنسية-، والجرائم ضد المصالح الحكومية. ويلاحظ أن التقسيم يقوم على فكرة

الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء، لكنه ليس تقسيماً منضبطاً ولا هو تقسيم محدد الأطر، فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة والاحتيال، أما الجرائم التي تستهدف التزوير فتمس الثقة والاعتبار، والجرائم الواقعة ضد الآداب قد تتصل بالشخص، وقد تتصل بالنظام والأخلاق العامة، وعلى العموم فإنه وتبعاً لهذا التقسيم الوارد ضمن مشروع القانون النموذجي الأمريكي - تصنف جرائم الكمبيوتر على النحو الآتي:

١- **طائفة الجرائم التي تستهدف الأشخاص:**

وتضم طائفتين رئيستين هما:

أ- الجرائم غير الجنسية التي تستهدف الأشخاص، وتشمل القتل بالكمبيوتر، والتسبب بالوفاة، جرائم الإهمال المرتبط بالكمبيوتر، والتحريض على الانتحار، والتحريض القصدي للقتل عبر الإنترنت، والتحرش والمضايقة عبر وسائل الاتصال المؤتمنة، والتهديد عبر وسائل الاتصال المؤتمتة، والأحداث المتعمد للضر العاطفي أو التسبب للضرر عاطفي عبر وسائل التقنية، والملاحقة عبر الوسائل التقنية، وأنشطة اختلاس النظر أو الإطلاع على البيانات الشخصية، وقنابل البريد الإلكتروني، وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب به، وبث المعلومات المضللة أو الزائفة، والانتهاك الشخصي لحرمة كمبيوتر (الدخول غير المصرح به).

ب- طائفة الجرائم الجنسية: وتشمل حض وتحريض القاصرين على أنشطة جنسية غير مشروعة، وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية، وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة، وتلقي أو نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة، والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية، ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام والقاصرين تحديداً، ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الإنترنت، وتصوير أو إظهار القاصرين ضمن أنشطة جنسية، واستخدام الإنترنت لترويج الدعارة بصورة قسرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم، والحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية.

بيد أننا عندما نمعن النظر في هذه الأوصاف نجد أنها تجتمع جميعاً تحت صورة واحدة هي استغلال الإنترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة.

٢- طائفة جرائم الأموال - عدا السرقة- أو الملكية المتضمنة أنشطة الاختراق والإتلاف:

تشمل أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة إمّا مجرداً أو لجهة ارتكاب فعل آخر ضد البيانات والبرامج والمخرجات، وتخريب المعطيات والممتلكات ضمن مفهوم تخريب الكمبيوتر، وإيذاء الكمبيوتر، واغتصاب الملكية، وخلق البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات، واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص، وإدخال معطيات خاطئة أو مزورة إلى نظام كمبيوتر، والتعديل غير المصرح به لأجهزة ومعدات الكمبيوتر، والإتلاف غير المصرح به لنظم الكمبيوتر (مهام نظم الكمبيوتر الأدائية)، وأنشطة إنكار الخدمة أو تعطيل أو اعتراض عمل النظام أو الخدمات، وأنشطة الاعتداء على الخصوصية (وهذه تخرج عن مفهوم الجرائم التي تستهدف الأموال لكنها تتصل بجرائم الاختراق) وإفشاء كلمة سر الغير، والحيازة غير المشروعة للمعلومات، وإساءة استخدام المعلومات، ونقل معلومات خاطئة.

٣- جرائم الاحتيال والسرقة:

تشمل جرائم الاحتيال بالتلاعب بالمعطيات والنظم ، واستخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص أو تدميرها، والاختلاس عبر الكمبيوتر أو بواسطته، وسرقة معلومات الكمبيوتر، وقرصنة البرامج، وسرقة خدمات الكمبيوتر (وقت الكمبيوتر)، وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر.

٤- جرائم التزوير:

تشمل تزوير البريد الإلكتروني، وتزوير الوثائق والسجلات، وتزوير الهوية.

٥- جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب:

تتضمن تملّك وإدارة مشروع مقامرة على الإنترنت، وتسهيل إدارة مشاريع القمار على الإنترنت، وتشجيع مشروع مقامرة عبر الإنترنت، واستخدام الإنترنت لترويج الكحول ومواد الإدمان للقصر.

٦- جرائم الكمبيوتر ضد الحكومة:

تشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون، والإخفاق في الإبلاغ عن جرائم الكمبيوتر، والحصول على معلومات سرية، والأخبار الخاطئة عن جرائم الكمبيوتر، والعبث بالأدلة القضائية أو التأثير فيها، وتهديد السلامة العامة، وبث البيانات من مصادر مجهولة، كمال تشمل السلامة العامة، وبث البيانات من مصادر مجهولة، كما تشكل الإرهاب الإلكتروني، والأنشطة النارية الإلكترونية أو أنشطة تطبيق القانون بالذات.(٢٤)

رابعاً: تصنيف جرائم الحاسب إلى فئات وفق بعض القوانين الأمريكية:

لقد جاء التصنيف السابق من بيئة أمريكية، كذلك فإن هذا التصنيف هو الآخر من بيئة أمريكية، إلا أنه يتضمن معطيات جديدة من حيث تناوله لجرائم تكنولوجيا المعلومات، ووفق هذا المعيار يمكن تصنيف جرائم الحاسب إلى فئات حسبما اعتبرته قوانين بعض الولايات الأمريكية داخلاً ضمن جرائم الحاسب، وكما يلي:

١- الوصول غير المرخص لنظام الحاسب: يشير الوصول غير المرخص لنظام الحاسب الآلي في هذا السياق إلى التفاعل مع النظام، أو استرجاع معلومات منه، أو تخزين بيانات فيه، أو استخدام وسائل الاتصالات للاتصال بنظام آخر.

٢- سرقة خدمات الحاسب الآلي: تحدث سرقة خدمات الحاسب عندما يستخدم فرد دون إذن مسبق نظاماً يخص فراداً أو جهة أخرى كاستخدام موظف في مؤسسة حاسب تلك المؤسسة لأداء أعمال تخص مؤسسة أخرى أو تخصه هو.

٣- العبث بعمليات الحاسب الآلي: يشمل هذا النوع من جرائم الحاسب أي نشاط لا يستند إلى تفويض يهدف إلى التلاعب بعمليات الحاسب أو إيقافها، أو منع مستفيدين مفوضين من خدمات الحاسب الآلي كزرع قنبلة زمنية موقوتة تؤدي إلى إيقاف عمليات النظام في حال توفر شروط محددة.

٤- إساءة استخدام المعلومات المخزنة بالحاسب الآلي: ويحدث هذا النوع من جرائم في حالة الكشف غير المفوض للمعلومات المخزنة، أو استخدامها، أو تغييرها، أو إتلافها.

٥- التحايل الحاسبي (computer Fraud) يعني هذا النوع التحايل باستخدام الحاسب الآلي كاستخدام الحاسب في مطالبة شركة التأمين والحصول على فائدة من جراء ذلك.

٦- سرقة أجهزة الحاسب الآلي وملحقاتها أو تدميرها.

٧- حجب الخدمة عن مواقع الإنترنت (denial of service) وذلك باستغلال حاسبات طرف ثالث لإرسال كمية هائلة من البيانات إلى المواقع المستهدفة بحيث يستحيل على المستخدمين الآخرين الدخول إلى تلك المواقع، وأكبر المواقع المستقلة، ومواقع البيع بالتجزئة مثل باي إنك (buy. Com)، وإبي إنك (ebay .com) وأمازون (amazon.com)، وسي إن إن (cnn.com) أيام الإثنين إلى الأربعاء من ٧-٢٠٠٠/٢/٩.

٨- نشر معلومات (نص أو صورة أو صوت) على الإنترنت كفرية أو مخلة بالدين أو منتهكة لحقوق الأفراد والجماعات التي ضمنها الإسلام.

٩- التطفل على مواقع الإنترنت. وتتعرض مواقع الإنترنت لأربعة أنواع من المتطفلين وهم:

أ- متطفل يريد أن يرى مكنون موقعك لمجرد الرؤية وإشباع رغبة الفضول فقط.

ب- متطفل يريد أن يرى مكنون موقعك ويغير معلوماته أو يلغيها أو حتى يبيعها للآخرين.

ج- متطفل يريد أن يستخدم موقعك كأداة هجوم على موقع آخر أكثر أهمية وأماناً من موقعك مما يحمّلك عواقب تدمير ذلك الموقع في حالة تدميره.

د- متطفل يريد أن يستخدم موقعك لنشر المعلومات التي يعاقب عليها القانون كبيانات الشركات السرية أو حتى صفحات العري وتجارة الجنس بشكل عام.(٢٥).

خامساً: تصنيف الجرائم كجرائم الكمبيوتر وجرائم الإنترنت:

يجري في نطاق هذا المعيار التمييز بين الأفعال التي تستهدف المعلومات في نطاق الكمبيوتر ذاته - خلال مراحل المعالجة والتخزين والاسترجاع - وبين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، وطبعاً الأنشطة التي تستهدف مواقع الإنترنت وخوادمها من نظم الكمبيوتر الكبيرة والعملاقة أو تستهدف تطبيقات واستخدامات وحلول الإنترنت وما نشأ في بيئتها من أعمال إلكترونية وخدمات إلكترونية.

نجد في إطار هذه الرؤية، أن البعض يحصر أنشطة جرائم الإنترنت بتلك المتعلقة بالاعتداء على المواقع وتعطيلها أو تشويهها أو تعطيل تقديم الخدمة (أنشطة بعنصري الموفورية والتكاملية أو سلامة المحتوى)، وكذلك أنشطة المحتوى الضار، كترويج المواد الإباحية والمقامرة، وأنشطة إثارة الأحقاد والتحرش والإزعاج ومختلف صور الأنشطة التي تستخدم البريد الإلكتروني والمراسلات

الإلكترونية، وأنشطة الاستيلاء على كلمات سر المستخدمين والهوية ووسائل التعريف، وأنشطة الاعتداء على الخصوصية عبر جمع المعلومات من خلال الإنترنت، وأنشطة احتيال الإنترنت كاحتيال المزادات وعدم التسليم الفعلي للمنتجات والخدمات، وأنشطة نشر الفايروسات والبرامج الخبيثة عبر الإنترنت، وأنشطة الاعتداء على الملكية الفكرية التي تشمل الاستيلاء عليها أو استخدامها خلافاً لحماية العلامة التجارية وأنشطة الاعتداء على محتوى المواقع والتصميم، وأنشطة الروابط غير المشروعة وأنشطة الأطر غير المشروعة (وهي أنشطة يقوم من خلالها أحد المواقع بإجراء مدخل لربط مواقع أخرى أو وضعها ضمن نطاق الإطار الخارجي لموقعه هو، وغيرها من الجرائم التي يجمعها مفهوم (جرائم الملكية الفكرية عبر الإنترنت).

أما جرائم الكمبيوتر فإنها وفق هذا التقسيم تعاد إلى الأنشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر وتحديداً أنشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الحاسوب ، واعتراض المعطيات خلال النقل (مع أنه مفهوم يتصل بالشبكات أكثر من نظم الكمبيوتر) إضافة للتدخل غير المصرح به والذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به لنظام الكمبيوتر ودخول مصرح به للشبكات فيتبع لمفهوم جرائم الإنترنت .(٢٦)

يبقى وبغض النظر عن نوع التصانيف السابقة الذكر لابد من القول: إن تلك التصانيف جاءت بمعايير مختلفة مرة ومتطابقة مرات أخرى، وهذا الاختلاف والائتلاف بالتأكيد نابع من وجهات نظر مختلفة سواء كانت قانونية أم اجتماعية أم نفسية أم أمنية.. الخ.

وفوق هذا وذاك ، أن تلك التصانيف وضعت أمام القارئ والمهتم بشؤون المجتمع أغلب الرؤى والتصورات لنوع من الجرائم لم يألفه المجتمع الإنساني من قبل، لاسيما المجتمع الذي سبق مجتمع المعلومات العالمي الحالي، وفي ذات الآن يدعو أفراد مجتمع المعلومات العالمي إلى أخذ العلم والحيطة والحذر من الوقوع بشرك جرائم تكنولوجيا المعلومات بقصد أم بغير قصد.

أخيراً لا بد من القول أيضاً: إن الحديث عن والتصانيف المختلفة وذكرها، وربما ذكر عددها لم يتوقف عند هذا الحد، بل سيتجاوزه مستقبلاً إلى أكثر من ذلك؛ وذلك مرده إلى أن تكنولوجيا المعلومات لم تصل بعد إلى مرحلة النضوج النهائي، فهي (أي تكنولوجيا المعلومات) ما زالت تكتب تاريخها الذهبي، وطالما الأمر كذلك، فإن جرائم تكنولوجيا المعلومات لم تصل إلى صيغها وأنواعها النهائية، ولا إلى طرق وأساليب ارتكابها النهائية، ولذلك فإن طرق تقسيمها

وتصانيفها لم تصل بعد على درجتها النهائية، ولهذا وذاك لم نضع هنا تصنيفاً جديداً على الأقل يمثل وجهة نظرنا، هذا من جهة، ومن جهة أخرى نرى أن التصانيف والتقسيمات الموجودة على الساحة المعرفية وافية بالغرض لحد الآن.

٧- خصائص وسمات جرائم تكنولوجيا المعلومات:

مثلما للجرائم العادية خصائص وصفات تتسم، فإن الأمر ينطبق كذلك على جرائم تكنولوجيا المعلومات، وتعد الجرائم التي ترتكب من خلال الحاسوب وشبكة الإنترنت هي جرائم ذات خصائص (CHARACTERISTICS) متفردة خاصة بها لا تتوافر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها والتي ترتكب يومياً في كافة دول العالم والتي لها خصائص أخرى مغايرة تماما لخصائص تلك الجرائم التي ترتكب عبر الحاسوب والإنترنت وتلك الخصائص الخاصة بجرائم تكنولوجيا المعلومات هي:

١- الحاسب الآلي هو أداة ارتكاب جرائم الإنترنت:

خاصية أن الحاسب الآلي (computer) هو دائماً أداة الجريمة في الجرائم التي ترتكب على شبكة الإنترنت هي خاصية متفردة عن أي جريمة أخرى؛ ذلك أن الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الإنترنت (internet) وقيامه بتنفيذ جريمته أياً كان نوعها، وعليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الإنترنت.

٢- الجرائم ترتكب عبر شبكة الإنترنت:

تعد شبكة الإنترنت (internet) هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات الصناعية وغيرها من الأهداف التي ما تكون غالباً الضحية لتلك الجرائم وهو ما دعا معظم تلك الأهداف على اللجوء غلى نظم الأمن الإلكترونية في محاولة منها لتحمي نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم.

٣- مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي:

لاستخدام الحاسب الآلي من أجل ارتكاب أو تنفيذ جريمة ما على شبكة الإنترنت لا بد وأن يكون مستخدم هذا الحاسب الآلي على دراية ومعرفة فائقة، وذو خبرة كبيرة في مجال استخدامه وإلا فأين له بالخبرة اللازمة التي تمكنه من تنفيذ جريمته والعمل على عدم إكتشافها

ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي وأن الشرطة تبعث أول ما تبحث عن خبراء الكومبيوتر عند ارتكاب الجرائم.

٤- **الجريمة لا حدود جغرافية لها:**

شبكة الانترنت ألغت أي حدود جغرافية فيما بين الدول وبعضها إذ يمكن التحدث فيما بين أشخاص ليس في بلدان مختلفة وإنما في قارات مختلفة في نفس الوقت على شبكة الإنترنت من خلال الدردشة (SHATINC) وعليه فإنه أي جرائم ترتكب عبر شبكة الإنترنت فإنها تتخطى حدود الدولة التي ارتكب فيها لتتعدى آثارها كافة البلدان على مستوى العالم (٢٧).

٥- جرائم الكمبيوتر والإنترنت طائفة من الجرائم التي تتسم بسمات مخصوصة عن غيرها من الجرائم، فهي تستهدف معنويات وليست ماديات محسوسة، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي إن جاز التعبير.

٦- كما أنها تتسم بالخطورة البالغة نظراً لأغراضها المتعددة، ونظراً لحجم الخسائر الناجم عنها قياساً بالجرائم التقليدية، ونظراً لارتكابها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمراً صعباً، ونظراً لأنها بذاتها تنطوي على سلوكيات غير مألوفة، وبما أتاحته من تسهيل ارتكاب الجرائم الأخرى تمثل إيجاد وسائل تجعل ملاحقة الجرائم التقليدية أمراً صعباً متى ما ارتكبت باستخدام الكمبيوتر.

٧- تحقيق وتحري جرائم الكمبيوتر والإنترنت والمقاضاة في نطاقها تنطوي على مشكلات وتحديات إدارية وقانونية تتصل ابتداءً بمعيقات ومتطلبات عمليات ملاحقة الجناة، فإن تحققت مكنة الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم. ونظراً لأنها جرائم لا تحدها حدود وتعد من الجرائم العابرة للحدود، فتثير لذلك تحديات ومعيقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

إن جرائم الكمبيوتر قد ترتكب عن طريق حاسب آلي في دولة ما، في حين يتحقق الفعل الإجرامي في دولة أخرى، فجرائم الكمبيوتر والإنترنت، لا تحدها حدود ولا تعترف ابتداءاً في هذه المرحلة من تطورها بسبب شبكات المعلومات – بعنصر المكان أو حدود الجغرافيا، وتتميز بالتباعد الجغرافي بين الفاعل والمجني عليه، ومن الوجهة التقنية، بين الحاسوب أداة الجريمة،

وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه وبفعل سيادة تقنيات شبكات النظم والمعلومات، امتد خارج هـذه الحـدود - دون تغيـير في الاحتياجات التقنية- ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء.

الحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر المسائل التي تثير إشكالات في مجال جـرائم الحاسوب وبشكل خاص الإجراءات الجنائية والاختصاص والقانون والواجب والتطبيق. وهذا بدوره عامـل رئـيس في نمـاء دعوات تظافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه الـسمة تـذكرنا بإرهاصـات جـرائم المخـدرات والاتجـار بالرقيق وغيرها من الجرائم التي وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلاً دون نجاعة أسـاليب مكافحتها، فلم يكن من بد غير الدخول في سلسلة اتفاقيات ومعاهدات

ولية لمكافحة هذه الجرائم، وذات الأمر يقال الآن بشأن أنشطة غسل الأموال، وهي في ذات الوقـت الأسـباب ذاتهـا التي تجعل موضوع جـرائم الإرهـاب والجـرائم المنظمـة والجـرائم الاقتـصادية المواضـيع عـلى أجنـدة اهـتمام المجتمـع الدولي.(٢٨)

٨- أسباب انتشار جرائم تكنولوجيا المعلومات:

بات مؤكداً يمكن القول: إن تزايد عدد أنواع أجهزة تكنولوجيا المعلومات جعل من الجرائم المرتبطة بها هي الأخرى في تزايد، بل وفي تنوع طرق ارتكابها، ويقف وراء ذلك التنوع والتنوع عدد من الأسباب.

إن من أهم أسباب انتشار جرائم الحاسب الآلي صـعوبة اكتـشاف هـذه الجريمـة ومقاضـة المـتهم لأنـه لا يوجـد في أغلب الأحوال شاهد للقضية ولا دلائل يمكن استخدامها للتوصل إلى الجانب. وقد يستهان في هذه الجـرائم أو يـركن إلى السكوت عنها، حيث إن كثيراً من المنشآت التي تخترق نظم معلوماتها لا تلاحق مرتكبي هـذه الجـرائم قـضائياً مفـضلة استقالتهم من أعمالهم - إن كانوا من داخل المنشأة - دون إثارة ضجة لئلا تشوه سمعة المنـشأة. ويحـاول العديـد مـن مديري نظم المعلومات الإدارية التكتم على ما يحدث من جرائم ذات علاقة بالحاسب الآلي وعدم رفعهـا إلى المـستويات الإداريـة العليـا في المنـشأة، وتحـاول المـستويات العليـا أيـضاً إن تخفيهـا عـن مجلـس الإدارة، كـما أن مجـالس الإدارة يتجاهلونهـا إذا وصـلت إلـيهم ولا يوصـولها إلى المـساهمين، مـما أدى إلى إفـلات العديـد مـن القراصـنة مـن العدالـة وتشجيعهم على ارتكاب جرائم أخرى.

مما يزيد الأمر صعوبة التطور التقني السريع الذي يساعد القراصنة على كسر الحواجز واختراق النظم باستخدام تقنيات وبرامج أكثر تطوراً لم تؤخذ في الحسبان عند وضع إجراءات الحماية.

وقد سهل انتشار شبكة الإنترنت في الآونة الأخيرة على مستوى عالمي اختراق نظم المعلومات المرتبطة بالشبكة من قبل قراصنة المعلومات الذي يقبعون في أماكن بعيدة لم تكن تشكل خطراً في السابق لانعدام الوسيلة. ولاحظ "سكوت سارني" المسؤول عن مكافحة الجريمة على الإنترنت في وزارة العدل الأمريكية أن الكمبيوتر الموصول بشبكة الإنترنت أصبح سلاحاً لاقتراف هذه الجرائم في عالم بلا حدود. وأضاف أن شبكة الإنترنت تسهل الجريمة أيضاً على غرار دعارة الأطفال. واعترف "دوغلاس بيريت"، أحد المسؤولين في مركز الحماية من جرائم الحاسب الآلي التابع للشرطة الفدرالية الأمريكية بأنه لا يمكننا أن نتوقع كل شيء لأن تحديد الخطر أمر بالغ الصعوبة.

أضف على ذلك، أن غياب الأنظمة والقوانين الرادعة نظراً لجدة أو لحداثة هذه الجرائم على المجتمع أدت إلى انتشارها واستفحال خطرها مما ينجم عن عدم إلحاق العقوبات المناسبة بمن يقبض عليه من القراصنة، ويمكن أن يضاف على هذه الأسباب أيضاً ضعف الوعي بهذه الجرائم وأساليب ارتكابها وكيفية الحماية من أخطارها.(٢٩).

علاوة على ذلك، يمكن أن نضيف عدداً آخر من الأسباب وراء انتشار جرائم تكنولوجيا المعلومات منها:

١- الفرص المتزايدة: إن ازدياد عدد مستخدمي الحاسوب من ذوي المعرفة والمقدرة في اختراق البيانات نتيجة "لامركزية المعالجة"، الشبكات، الاتصالات والدخول عن بعد إلى الحاسوب قد اتخذت فرصاً متزايدة للمزورين والمتلاعبين لتنفيذ أغراضهم لاسيما في ظل سيطرة ورقابة غير كفوءة في هذا المحيط الإلكتروني لمعالجة البيانات.

٢- صعوبة الاكتشاف: إن وجود كم كبير من البيانات المخزنة في الحاسوب يجعل إخفاء أي تزوير أو تلاعب عملية سهلة خاصة إذا تمكن مرتكب الجريمة من عدم ترك أي دليل خلفه، الأم الذي يترتب عليه صعوبة اكتشاف الجريمة.

٣- تحقيق أرباح كبيرة: نتيجة للأرباح الطائلة التي يمكن أن يجنيها مرتكب التزوير والتلاعب، فإنها تشكل دافعاً قوياً لأصحاب النوايا السيئة في ارتكاب جريمتهم في

استبيان أجراه أحد الباحثين في أمريكا عام (١٩٩٥) بيّن أن معدل أرباح مرتكب جريمة الحاسوب وصلت إلى "٦٠٠.٠٠٠" دولار مقابل "٣٠٠.٠٠٠" دولار لمرتكب الجريمة في النظام اليدوي.(٣٠).

٤- صعوبة الاحتفاظ الني بآثارها إن وجدت.

٥- إنها تحتاج إلى خبرة فنية وتقنية ويصعب على المحقق التقليدي التعامل معها.

٦- إنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

٧- إنها تعتمد على قمة الذكاء والمهارة في ارتكابها.(٣١).

٨- الولع في جمع المعلومات وتعلمها:

فهناك من يقوم بارتكاب جرائم الكمبيوتر بغية الحصول على الجديد في المعلومات. فيرى قراصنة الكمبيوتر أن الحصول على المعلومة يجب ألا يكون عليه أي قيد. فالقرصان يوطّد كل جهده في تعلم كيفية اختراق المواقع الممنوعة. وغالباً ما يكون القراصنة مجموعات يكون الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والأخبار. ويفضل القراصنة أن يكونوا مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول فترة ممكنة.

٩- الدوافع الشخصية:

غالباً ما يرتكب المبرمج جرائم الكمبيوتر نتيجة احساسه بالقوة والذات وبقدرته على اقتحام النظام فيندفع تحت تأثير الرغبة القوية في تحقيق الذات ومن أجل تأكيد قدرته الفنية على ارتكاب أحد جرائم الكمبيوتر. وقد يكون الهدف من ارتكاب الجريمة الحقد والكراهية، فقد دفع الانتقام بمحاسب شاب إلى أن يتلاعب في برامج الكمبيوتر الخاصة بالشركة التي يعمل بها، حيث برمجها إلى أن تختفي كل البيانات الخاصة بديون الشركة بعد مضي ستة أشهر من تاريخ تركه للعمل وحدث ما أراد بالفعل. فبعد أن ترك العمل ومرت ستة أشهر اختفت البيانات الخاصة بديون الشركة نهائياً من على جهاز الكمبيوتر، وقد يكون الدافع الشخصي لمرتكب جرائم الكمبيوتر دافع مذهبي ومن أمثلة ذلك:

ما تقوم به جماعات الألوية الحمراء في ايطاليا، حيث تعرضت عدة وزارات وجماعات ومؤسسات مالية في إيطاليا لهجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها. ولقد أصدرت هذه الجماعة منشور عام ١٩٨٨، شرحت فيه إستراتيجيتها وأغراضها

وأهدافها، ويبدأ المنشور بتحديد أهداف هذه الجماعة وهي مهاجمة الهيئات متعددة الجنيات التي ترمز للامبريالية، وإعادة توزيع الحركة الثورية بتنظيم من الحزب الشيوعي المحارب، ويقصد بالهيئات متعددة الجنسيات تلك الموجودة بالولايات المتحدة الأمريكية ويعتبرون الكمبيوتر سلاح خطير ضد الإرهاب بفضل قدرته على حفظ المعلومات.

١٠- المؤثرات الشخصية:

من المعلوم أن البرامج والمعلومات المخزنة داخل جهاز الكمبيوتر لها قيمة مادية كبيرة بغض النظر عن قيمة المادة المخزنة عليها سواء كانت (سي دي أو دسك)، فهذه البرامج أو المعلومات ذات قيمة مالية مرتفعة، لذلك تسعى بعض الشركات التجارية والصناعية إلى الحصول على هذه البرامج والمعلومات عن طريق سرقتها بواسطة القائمين على أجهزة الكمبيوتر، وغالباً ما يقوم بذلك مقابل رشوة الموظف أو إغرائه أو خداعه أو استغلال نقاط ضعفه.

١١- حب المغامرة والإثارة:

جاء على لسان أحد القراصنة في كتاب (قراصنة أنظمة الكمبيوتر)، كانت القرصنة هي النداء الأخير الذي يبعثه دماغي. فقد كنت أعود إلى البيت بعد يوم عمل ممل في المدرسة، وأدير تشغيل جهاز الكمبيوتر وأصبح عضواً في نخبة قراصنة الأنظمة، وكان الأمر مختلف برمته، حيث لا وجود لعطف الكبار ، وحيث الحكم هو لموهبتك فقط. في البدء كنت أسجل اسمي في لوحة النشرات الخاصة، حيث يقوم الأشخاص الآخرين الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد، وبعد ذلك أبدا عملية القرصنة الفعلية وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة، وأتنقل من جهاز كمبيوتر إلى آخر محاولاً العثور على سبيل للوصول إلى هدفي. وكان يرافق ذلك تزايد سرعة الأدرينالين. وكل خطوة أخطوها كان يمكن أن تسقطي بيد السلطات. كنت على حافلة التكنولوجيا واكتشاف ما ورائها، واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجودي بها. (٣٢).

هوامش الفصل الثالث:

١- الشبكة القانوني العربية - فرع القانون، جرائم الكمبيوتر والإنترنت. منشور على موقع Arabi@wNet- Lawsubjects. تم زيارته بتاريخ ٢٠٠٤/١١/١٢.

٢- المرجع السابق نفسه.

٣- Robert Irvine smith and Bob compbell. Information Technology Revolution- York, Yorkshire, Britain: Iongman, ١٩٨١.P.I.\

٤- عبد الفتاح بيومي حجازي: الأحداث والإنترنت: دراسة متعمقة عن أثر الإنترنت في انحراف الأحداث- الإسكندرية: دار الفكر الجامعي، ٢٠٠٢. ص ٣٦.

٥- هدى حامد قشقوش. جرائم الحاسب الإلكتروني في التشريع المقارن - القاهرة : دار النهضة العربية، ١٩٢، ص٢٠.

٦- سليمان مصطفى أبكر: جرائم الحاسب الآلي وطرق المواجهة. مجلة الأمن والحياة، ع ٢٤٣، السنة الحادية والعشرون (أكتوبر/ نوفمبر) - الرياض: أكاديمية نايف للعلوم الأمنية، ٢٠٠٢. ص ٥٠.

٧- Merwe vander . computer crimes and other crimes against information Techndogy in south Africa. R.I.D.P, ١٩٩٣, P. ٥٥٤.

٨- سامي الشوا: الغش المعلوماتي كظاهرة إجرامية مستحدثة في المؤتمر السادس للجمعية المصرية للقانون الجنائي- القاهرة: الجمعية المصرية للقانون الجنائي، ١٩٩٣، ص٢.

٩- عادل عبد الجواد محمد. إجرام الإنترنت. مجلة الأمن والحياة، ع٢٢١ (ديسمبر/ يناير)، ٢٠٠١. ص ٧٠.

١٠- محمد أمين أحمد الشوابكة: جرائم الحاسوب والإنترنت: الجريمة المعلوماتية - عمّان: مكتبة دار الثقافة، ٢٠٠٤. ص ١٥.

١١- طارق قابيل: برامج الكمبيوتر في دور "القاتل الندل". تكنولوجيا المعلومات والاتصالات - إسلام أون لاين . نت. ٢٠٠٢.

١٢- ستفين أ. موسكوف:ه مارك ج. سيمكن . نظم المعلومات المحاسبية لاتخاذ القرارات: مفاهيم وتطبيقات ، ترجمة كمال الدين سعيد، أحمد حامد حجاج- الرياض: دار المريخ، ٢٠٠٢. ص ٤٦٥.

١٣- الشبكة القانونية العربية - فرع القانون. جرائم الكمبيوتر والإنترنت: المعنى والخصائص والصور واستراتيجية المواجهة القانونية Arabi@wNet-Lawsubiects، تم زيارته بتاريخ ٢٠٠٤/١١/١٤. ص ١١.

١٤- طارق قابيل. مرجع سابق.

١٥- صالح بن محمد المسند، عبد الرحمن بن راشد المهيني: جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات- المجلة العربية للدراسات الأمنية والتدريب، م١٥ـ غ٢٩ - الرياض: أكاديمية نايف العربية، ٢٠٠٠. ص ١٥٠-١٥١.

١٦- الشبكة القانونية - فرع القانون. مرجع سابق. ص ١١-١٢.

١٧- طارق قابيل: مرجع سابق.

١٨- الشبكة القانونية- فرع القانون- جرائم الكمبيوتر والانترنت- مرجع سابق ص ٩-١٠.

١٩- ستيفن أ. موسكوف، مارك ج- سيمكن. مرجع سابق. ص ٤٥٦-٤٥٨.

٢٠- الشبكة القانونية - فرع القانون- جرائم الكمبيوتر والانترنت. مرجع سابق. ص ١٢-١٥.

٢١- سليمان مصطفى أبكر. مرجع سابق. ص ٥٠.

٢٢- الشبكة القانونية - فرع القانون- جرائم الكمبيوتر والانترنت. مرجع سابق. ص ١٦.

٢٣- صالح بن محمد المسند، عبد الرحمن بن راشد المهيني. مرجع سابق ص ١٨١.

٢٤- الشبكة القانونية - فرع القانون- جرائم الكمبيوتر والانترنت. مرجع سابق. ص ٢١-٢٤.

٢٥- صالح بن محمد المسند ، عبد الرحمن بن راشد الميهني. مرجع سابق ص ١٧٩-١٨١.

٢٦- الشبكة القانونية - فرع القانون- جرائم الكمبيوتر والانترنت. مرجع سابق. ص ٢٥.

٢٧- منير محمد الجنيهي: ممدوح محمد الجنيهي. جرائم الإنترنت والحاسب ووسائل مكافحتها- الإسكندرية: دار الفكر الجامعي، ٢٠٠٤. ص ١٤-١٥.

٢٨- الشبكة القانونية - فرع القانون- جرائم الكمبيوتر والانترنت. مرجع سابق. ص ٣٣.

٢٩- صالح بن محمد المسند: عبد الرحمن بن راشد الميهني. مرجع سابق ص ١٧٥-١٧٦.

٣٠- سرحان سليمان السرحان: محمود عبد المنعم المشهداني. أمن الحاسوب والمعلومات- عمّان: دار وائل، ٢٠٠١، ص ١١٥-١١٦.

٣١- منير محمد الجنبيهي: ممدوح محمد الجنبيهي. مرجع سابق . ص ١٩.

٣٢- محمد أمين الرومي: جرائم الكمبيوتر والإنترنت - الإسكندرية: دار المطبوعات الجامعية، ٢٠٠٤، ص ٢٣-٢٦.

الفصل الرابع




جرائم تكنولوجيا المعلومات مقترفوها، أساليب ارتكابه، أنواعها.

تقديم:

لقد أصبح موضوع ظاهرة جرائم تكنولوجيا المعلومات محور اهتمام العديد من المهتمين بشؤون المجتمعات، بيد أن الأمر بالنسبة لعامة الناس لا زال يكتنفه الغموض والالتباس، لاسيما عن أولئك الذين ينفذون هذه الجرائم، فالعديد من عامة الناس يسألون عن: من هم الأشخاص الذي يقومون بمثل هذه الأعمال الإجرامية؟ وما الوسائل والطرق التي تتبع في ارتكاب هذا النوع من الجرائم؟ كذلك يتساءل بعضهم عن أنواع جرائم تكنولوجيا المعلومات وما طبيعة هذه الجرائم؟ كل هذه الأسئلة والتساؤلات أصبحت حقاً مثيرة، بل تبرز حقيقة لا يمكن تجاهلها أو إغفالها تلك التي تتعلق بحاجة الناس الماسة إلى توفير الأمن للمجتمع من مخاطر جرائم تكنولوجيا المعلومات، والأمن في هذا الجانب لا يتأتى إلا من خلال التعرف على ماهية هذه الجرائم، ومن ثم أنواعها، ومن يرتكبها، والوسائل والأساليب والطرق التي يتم استخدامها لتنفيذ هذا النوع من الجرائم، وذلك كله يتأتى من خلال إجراء العديد من الأبحاث والدراسات في هذا المجال، وهذا الفصل يسلط الضوء على كل النقاط التي يمكن أن تشكل حالة الوعي لدى أفراد المجتمع. فلنتبين من ذلك.

١- من الذي يرتكب جرائم تكنولوجيا المعلومات؟

أ- مواصفات مرتكبو جرائم تكنولوجيا المعلومات.

حدّد " دون باركر" الخبير بجرائم الحاسوب، مواصفات مرتكب جريمة الحاسوب، وحدّدها في ثلاثة شروط يجب أن تتوافر جميعها في شخص واحد، ولكن وبسبب التطورات التكنولوجية التي حصلت مؤخراً والتوسع في استخدام الحاسوب فقد تزايدت أعداد الذين يمتلكون هذه المواصفات، والتي تمكنهم من اختراق الحاسوب وارتكاب جريمتهم في التزوير، وقد حدد "باركر" هذه الصفات بالآتي:

١. المعرفة: (knowledge):

مع انتشار استخدام الحاسوب الشخصي ازداد عدد مستخدميه، ومعها ازداد عدد ذوي العلم والمعرفة ولاسيما المعرفة بنقاط الضعف في الأنظمة المطبقة عليه مما يشجع ويسهل ارتكاب جريمة الحاسوب.

٢. القدرة على اختراق وسائل الخزن: (Access):

نتيجة للتوجه الحاصل نحو اللامركزية في المعالجة بواسطة الحاسوب فقد ازداد استخدام الشبكات ووسائل الاتصال من أجل التفاعل عن بعد مع الحاسوب الأمر الذي أدى إلى ازدياد

أعداد المستخدمين، وبتوفير المعرفة المناسبة فلن يجد المستخدم صعوبة في استغلال وسائل الاتصال من أجل الوصول إلى مواقع خزن البيانات وتنفيذ جريمته لاسيما إذا لم تكن وسائل الخزن محاطة بنظام كفؤ للحماية.

٣. القابلية على استخدام الوسائل: (Resources):

مع تزايد وسائل الاتصال بالحاسوب وتزايد أعداد ذوي المعرفة به، تهيأت الظروف لأصحاب النوايا السيئة في استغلال وسائل الاتصال هذه وغيرها من مصادر الحاسوب سواء ما يتعلق منها بالخزن أو المعالجة لتنفيذ جريمة الحاسوب.

قد يكون السؤال المهم هنا مفاده من أين يتم ارتكاب الجريمة الإلكترونية من داخل البلد أم من خارج أسوار الوطن؟ يمكن أن يكون مرتكب الجريمة من داخل المؤسسة أو من خارجها، وهذا يعني ممكن أن يكون المجرم من أبناء البلد أو من غيرهم (أجنبي)، ففي استبيان أجري في الولايات المتحدة الأمريكية والتي تعد من أكثر الدول التي تعاني من جرائم الحاسوب، وجد أن (٩٨%) من مجموع الجرائم نفذت من قبل أشخاص من داخل المؤسسة التي تعرضت للجريمة وهي تتمحور حول نوايا ودوافع مرتكبيها التي تشمل اختلاس الموجودات، السرقة وإتلاف البيانات، التضليل وتشويه الحقائق، وأن درجة الضرر الذي يمكن أن تسبب به الجريمة تعتمد بشكل رئيس على خبرة مرتكبيها.(١).

أضف على ذلك، صرح بعض خبراء مكافحة الجرائم بالكمبيوتر أن أفضل وسيلة للتعرف على الأشخاص ذوي الميول الإجرامية هي تحليل وتقييم مهاراتهم ومعرفتهم وخبرتهم الفريدة والتي تشبه تلك التي تميز مقترفي الجرائم بالكمبيوتر. فغالباً يكون مرتكب الجريمة قوي الذاكرة وذو موهبة غير عادية، وعلى درجة عالية من الذكاء وذو ثقافة راقية. ومن الغريب أن كل هذه الصفات والخصائص هي التي تؤهل هؤلاء الأفراد لشغل وظائف مرموقة في ميادين الكمبيوتر على درجة عالية من الذكاء ليس فقط لفهم ومعرفة نظام الكومبيوتر المختلفة، فمن الواضح أنه يجب أن يكون المختص في عمليات الكمبيوتر على درجة عالية من الذكاء ليس فقط لفهم ومعرفة نظام الكومبيوتر المستخدم، بل كذلك للتعرف على أوجه ضعف النظام حتى يمكنه وتخطيط تلاعبه؛ ولهذا السبب يعتبر الذكاء المرتفع والتعليم الراقي من أهم خصائص مرتكبي الجرائم بالكومبيوتر.

علاوة على ذلك فإن صفات مرتكبو جرائم تكنولوجيا المعلومات لم تقف عند هذا الحد، بل تزايدت إلى أكثر من ذلك، فالحقيقة الثانية عن مقترفي هذه الجرائم أن معظمهم من الرجال

الذين تقل أعمارهم عن ثلاثين عاماً، فمثلاً كان عمر (Schneider) وقت البدء في تنفيذ جريمته (١٩) عاماً، فإن تكنولوجيا الكمبيوتر تعتبر حديثة نسبياً ولم تُدرس هذه التكنولوجيا كما نعرفها الآن بالمدارس والجامعات إلا حديثاً، وقد يكون ذلك مؤشراً على صغر متوسط أعمال مقترفي هذه الجرائم. هذا بالإضافة إلى زيادة الحاجات المادية لهؤلاء الأفراد في هذه الفترة من العمر بجانب عدم تردد العديد منهم في الإقدام على المخاطرة في سبيل تحقيق مكاسب مادية.(٢)

ب- حسن الخلق أو خلقية غير إجرامية:

لا ينطبق ذلك المثال المعروف بأن (ليس للص أي أخلاقيات) على مرتكبي الجرائم بالكمبيوتر من وجهة نظرهم، فمعظمهم يعتبرون أنفسهم أشخاصاً أمناء يستخدمون الكومبيوتر فقط للحصول على ما يحصل عليه الآخرون من المستودعات. وعدد كبير منهم يعتبر نفسه مقترضاً لأجل طويل، وليس بلص، والعديد منهم تعمد تفادي الإضرار بأفراد آخرين خلال تنفيذ تلاعبهم. والرأي الشائع بين مرتكبي الجرائم بالكمبيوتر هو إيقاع الأضرار بالمؤسسة أو جهة غير محددة في استطاعتها اقتصادياً أن تتحمل عبء هذه الأضرار، لا الإضرار بالأفراد، كما أن البعض الآخر من أولئك المجرمين يعتبر هذه العمليات قضاءً وقدراً.

كانت الرغبة في التحدي في عدد من المواقف هي الوازع الرئيس للإقدام على اقتراف الجريمة باستخدام الكومبيوتر، وبهذا الشكل لا يعتبر التلاعب من خلال استخدام الكمبيوتر، وبهذا الشكل لا يعتبر التلاعب من خلال استخدام الكمبيوتر جريمة بل نوع من الألاعيب والجرائم ليس فيه أي مخالفات للمبادئ الأخلاقية. ويسود هذا النوع من الميول بين طلاب الجامعات الذين يسيئون استخدام أجهزة الكمبيوتر في جامعاتهم، هذا بالإضافة إلى بعض العمليات التجارية الأخرى.

كما أستند بعضهم في تبرير جرائمهم على انتشار أنواع خاصة من العمليات غير المشروعة في ميدان الكمبيوتر واستخداماته. فيعتبر التحريف أو العبث في برامج الكمبيوتر التي تستخدمها البنوك مخالفة قانونية في حد ذاتها، ولكن مثل هذا العمل متبعاً وجارٍ أداؤه بصفة عامة من أجل محاولة تنفيذ وإنجاز العمليات في التواريخ المحددة. ومن جهة أخرى اعترف أحد المتهمين، الذين قام بسرقة برامج وبيانات الكومبيوتر التي تحتفظ بها الشركة المنافسة للشركة التي يعمل فيها، من خلال محطة الاتصال المباشر واستخدام الرموز السرية، بأن سرقة ملفات وبرامج المنافسين ما هي إلا عمليات عادية يقوم بتنفيذها معديّ البرامج المتنافسين بغرض التجسس على أعمال الغير والحصول على المعلومات؛ ولذا أصاب أحد مقترفي هذه الجريمة الدهشة والإحساس بالإهانة وعدم الكرامة عندما صدر ضده حكم قضائي.

يتضح مما سبق: أن مرتكب الجريمة غالباً يكون شخصاً عادياً معتدل القيم والأخلاقيات، ولكن ذو حظ سيء في وظيفته. ولذا يتميز مرتكبو الجرائم بالكمبيوتر باعتقادهم بأن تلك الأصول التي يمكن التحكم فيها من خلال استعمال الكمبيوتر متاحة لهم، ولهم الحق في الحصول عليها حتى ولو لفترة مؤقتة لاستخداماتهم الشخصية (٣).

عندما يتم استقراء التاريخ الإجرامي للمجرمين من قبل المتخصصين في شؤون الجريمة والإجرام، لم يتم تصنيف المجرمين في مجال جرائم تكنولوجيا المعلومات من ضمن المجرمين، وقد تكون هذه القراءة قديمة نوعاً ما على الرغم من أن تاريخ جرائم تكنولوجيا المعلومات يعد حديثاً قياساً بالجرائم التقليدية، بيد أن الأمر بات مختلفاً عن السابق، فجرائم تكنولوجيا المعلومات باتت تشكل ظاهرة لافتة للأنظار، مما يجعل أن مرتكبيها هم يقعون ضمن فئات المجرمين إذا صحّ التعبير، لكن تبقى القراءات متباينة وهذا التباين متأتي من اختلاف وجهات المهتمين بشؤون ظاهرة جرائم تكنولوجيا المعلومات.

يعد الاستفسار عن ما إذا كان للشخص أي خبرات بعمليات إجرامية ذات أهمية عالية لتفادي إعطاء الفرصة لمنظمات الجرائم لتنفيذ مخططاتها في المؤسسات والشركات، ولم تشر أي دراسات حديثة إلى وجود أي علاقة بين منظمات الجرائم المنتشرة في أنحاء الولايات المتحدة الأمريكية والجرائم بالكمبيوتر، علماً بأن ذلك لا ينفي احتمال وجود حالات لم يكتشف أمرها بعد.

طبقاً لما أشار إليه المتخصصون، بأن معظم مرتكبي الجرائم بالكمبيوتر هواة وليسوا من محترفي الجريمة، وتعتبر هذه الجريمة أول جريمة لهم يقترفوها، فهناك قلة صغيرة جداً من مرتكبي تلك الجرائم يفتخرون بتلاعبهم أو أقروا بأن السرقة بالكمبيوتر هي مصدر دخلهم الوحيد. فعدد أولئك المحكوم عليهم في جرائم الكمبيوتر ولهم صحيفة سوابق صغيرة جداً، ولهذه الحقيقة أهمية بالغة عند توظيف أشخاص جدد للعمل في عمليات الكمبيوتر بالمؤسسة. كما أن اختيار المرشحين على أساس عدم وجود صحيفة سوابق لهم فقط غير كافٍ في الحسبان، منها على سبيل المثال: مدى الاستقرار الذهني والعقلي والاجتماعي والنفسي للشخص، والذي قد يؤثر على كيفية تصرف هذا الشخص مستقبلاً في ضوء ظروف العمل بالمؤسسة. وتشير التقارير والسجلات إلى ضرورة توخي الحذر عند توظيف أشخاص يتصفون بالسخط والاستياء معها اختلفت الأسباب والدواعي؛ لأن وجود موظف واحد مستاء نفسياً يمثل خطراً جسمياً على نظم المعلومات المحاسبية(٤).

ج- أصدقاء أم أعداء؟

عند استدعاء الماضي وقراءة سجل المجرمين، لا سيما في مجال جرائم تكنولوجيا المعلومات، يبرز في الحال سؤال مهـم مفاده: هل هناك ثمة أصدقاء في العالم الإلكتروني في ضوء خلقياتهم غير الإجرامية؟ يأتي الجواب فيخبر الجميع بأنه لـيس ثمة أصدقاء في العالم الإلكتروني، وصغير المجرمين ككبيرهم، والمازح من بينهم كالحاقد وضمان أمن المعلومات وضمان عدم التعرض للمسؤوليات يوجب التعامل مع الكل على أنهم مصدر للخطر، وليست المسألة إهداراً لفكرة حسن النية أو الثقة بالآخرين، إنها الضمان الوحيد للحماية من مصادر خطر بالغة قد تؤدي إلى مسؤوليات وخسائر لا يمكن تقديرها أو تجاوزها.

ما من شك أن المدى الزمني لنشأة وتطور العلوم الجنائية، حمل معه نشوء وتطور واندثار نظريات عدّة في مجال علم الإجرام، وفي مجال تصنيف المجرمين، وأسباب الجنوح والانحراف، وأمكن في ظل هذه العلوم، وما نتج في نطاقها من دراسات، في ميدان علم الإجرام تحديداً، بلورة سمات عامة للمجرم عموماً، وسمات خاصة يمكن استظهارها الطائفة معينة من المجرمين، تبعاً للجرائم التي يرتكبونها، فعلى سبيل المثال: أفرزت الجرائم الاقتصادية ما يعرف بإجرام ذوي الياقات البيضاء، وبالتالي كان طبيعياً أن تحمل ظاهرة جرائم الحاسوب في جنباتها ولادة طائفة من المجرمين، مجرمو الحاسوب، تتوافر فيهم سمات عامة بغض النظر عن الفعل المرتكب، وسمات خاصة تبعاً للطبيعة المميزة لبعض جرائم الحاسوب، والأغراض المراد تحقيقها. والحقيقة أنها وحتى الآن، لم تتضح الصورة جلية في شأن تحديد صفات مرتكبي الحاسوب، واستظهار سماتهم، وضبط دوافعهم، نظراً لقلة الدراسات الخاصة بالظاهرة برمتها من جهة. ونظراً لصعوبة الإلمام بمداها الحقيقي، بفعل الحجم الكبير من جرائمها غير المكتشفة ، أو غير المبلغ عن وقوعها، أو التي لم تتم بشأنها ملاحقة قضائية رغم اكتشافها، لصعوبة إثباتها أو للنقص التشريعي الذي يحد من توفير الحماية النائية في مواجهتها.

لم تكتمل الإجابة عن السؤال السابق والذي مفاده: من الذي يرتكب جرائم تكنولوجيا المعلومات؟ ربما تّم الإجابة عن جزء منه، بيد إن الجزء الآخر من الجواب يتعلق بتحديد هؤلاء المجرمين. ولكي تكتمل ملامح الإجابة عن السؤال، لا بد من القول: إنه وفي بداية الظاهرة شاع الحديث عن المجرمين الصغار الذي يرتكبون مختلف أنواع الإعتداءات على نظم الكمبيوتر وتحديداً الاختراقات بدافع التحدي وإثبات المقدرة العلمية والتقنية، وكان ثمة حديث عن استغلال منظمات الجريمة لهؤلاء النابغين وتحديداً استغلال ميول التحدي لديهم وأحياناً احتياجاتهم المادية

لتسخيرها للقيام بأنشطة جرمية تتصل بالتقنية تدر منافع لمنظمات الجريمة، ومع تنامي الظاهرة وتعدد أنماط هذه الجرائم، ونشوء أنماط جديدة متصلة بشبكات الكمبيوتر وتحديداً الإنترنت، اتجهت جهات البحث وتحديداً الهيئات العاملة في ميدان السلوك الإجرامي لمحاولة تصنيف مرتكبي جرائم الكمبيوتر والإنترنت وبيان السمات الأساسية لكل فئة بغرض بحث أنجح الوسائل لردع هذه الفئات أو الحد من نشاطها، باعتبار ذلك من المسائل الموضوعية اللازمة لتحديد اتجاهات المكافحة.

إنّ دراسات علم الإجرام الحديثة في ميدان التقنية تسعى في الوقت الحاضر إلى إيجاد تصنيف منضبط لمجرمي التقنية لكنها تجد صعوبة في تحقيق ذلك بسبب التغير السريع الحاصل في نطاق هذه الظاهرة والمرتبط أساساً بالتسارع الرهيب في ميدان الكمبيوتر والإنترنت، فالمزيد من الوسائل والمخترعات والأدوات التقنية يساهم في تغير أنماط الجريمة وتطور وفعالية وسائل الاعتداء، وهذا بدوره يساهم في إحداث تغيرات على السمات التي يتصف بها مجرمي التقنية، على الأقل السمات المتصلة بالفعل نفسه وليس بالشخص ولهذا يتجه الباحثون مؤخراً إلى الإقرار بأن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء وليس على أساس التكنيك الفني المرتكب في الاعتداء أو على أساس الوسائط محل الاعتداء أو المستخدمة لتنفيذه(٥).

لأجل تسليط الضوء على أنواع مجرمي تكنولوجيا المعلومات لا بد من استعراض أهم التصانيف بهذا الخصوص. ففي ندوة لوكالة حماية البرامج، بخصوص جرائم نظم المعلومات أو مرتكبي جرائم الحاسب، انتهت تلك الندوة إلى تصنيف لصوص تقنية المعلومات إلى المجموعات الآتية:

الأولى: وهي أكثر المجموعات رأفة ويمثلها طبقة من الشباب لديه قدر لا بأس به من الخبرة المعلوماتية، ويمارس مواهبه في المساء على الحاسب الآلي، بغرض الدخول في نظم المعلومات لأجل ممارسة الألعاب، وتدخل هذه الفئة - حسب رأينا - ضمن أحداث الجانحين.

الثانية: وهي من نفس نمط المجموعة السابقة، ولكن تتفوق عليها من حيث العلم والمعرفة بلغة البرمجة، وهدفها التسلية والملاحظة ، وهذه الفئة تدخل ضمن الأحداث الجانحين.

الثالثة: وهي أكثر المجموعات ضرراً، ولها كفاءة المجموعة السابقة، لكنها لا تكتفي بالملاحظة، بل تلجأ إلى أفعال الاعتداء الهمومي.

الرابعة: وهي أكثر المجموعات خطورة، ولها نفس هدف المجموعة السابقة- أي الإرهاب المعلوماتي - ولكن استخدام وسائل على قدر كبير من البراعة، كزرع برامج الفيروسات والقنابل المنطقية خلسة، والتي ينشأ عنها أضرار جسيمة (٦).

الخامسة: الموظفون الساخطون على مؤسساتهم الذين يعودون لمواقع العمل بعد فترات العمل الرسمية إما لغرض سرقة المعلومات أو بغرض التخريب.

السادسة: الموظفون العاملون بمراكز الحاسوب وهؤلاء يمثلون الغالبية العظمى من مرتكبي جرائم الحاسوب، وذلك لسهولة اتصالهم بالحاسوب.

السابعة: فئة العابثين (Hachers) هم الذين ليس لديهم سلطة استخدام الحاسوب ولكنهم مغرمون بالعبث وهم يستخدمون الحاسوب من أجل التسلية وليس بغرض التخزين وغالباً ما يكون من هواة الكمبيوتر.

الثامنة: الفئة التي تعمل في مجال الجريمة المنظمة باستخدام الحاسوب، حيث يقوم هؤلاء باستخدام الحاسوب في شكل غير قانوني في معرفة بعض الأشياء المتعلقة بالأساليب الأمنية المتبعة لتأمين المؤسسات التي يسطون عليها.

التاسعة : فئة صانعي ونشاري الفيروسات (sillaation of computer criminal viruses)(٧).

أما التصنيف الآخر لمجرمي تكنولوجيا المعلومات فهو الآتي:

١. المخترقون أو المتطفلون:

هذه الطائفة لدى هذا الرأي لا تختلف عن طائفة الهاكرز، علماً أن بين الاصطلاحين تبايناً جوهرياً، فالهاكرز متطفلون يتخذون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات المقدرة أما الكريكرز، فإن اعتداءاتهم تعكس ميولاً جرمية خطرة تنبئ عنها رغباتهم في إحداث التخريب، ومع أن هذا المعيار غير منضبط، إلا أن الدراسات والمعالجات في حقل جرائم الكمبيوتر والإنترنت، بل بعض التشريعات المحلية للهجمات الحاقدة والمؤذية في حين أن اصطلاح الهاكرز مرادف في الغالب لهجمات التحدي، طبعاً دون أن يؤثر هذا التمييز على مسؤولية مرتكبي الأنشطة من كلا الطائفتين ومساءلتهم عما يلحقونه من أضرار بالمواقع المستهدفة باعتداءاتهم. هذا إضافة إلى أن الاصطلاحيْن يختلفان واقعياً ومن حيث الأساس التاريخي لنشأة كل منهما. وأفراد هذه الطائفة يرتكبون جرائم التقنية بدافع التحدي الإبداعي ويجدون أنفسهم متفقين إلى درجة إلى أنهم

ينصبون أنفسهم أوصياء على أمن نظم الكمبيوتر في المؤسسات المختلفة، والسمة الغالبة على أعضاء هـذه الطائفـة صغر السن وقلة الخبرة وعدم التمييز بين الأنظمة محل الاختراق (طبعاً يتميز الكريكرز عن الهاكرز في مـستوى المعرفـة التقنية)، وبرغم هذه السمات فقد تمكن المجرمون من هذه الطائفة من اختراق مختلف أنـواع نظـم الكمبيـوتر التابعـة للشركات المالية والتقنية والبنوك ومصانع الألعاب والمؤسسات الحكومية ومؤسسات الخدمة العامة، وكثر الحـديث عـن وقائع عملية كما في حالة اختراق أحد الصبية الذي يبلغ من العمر (١٤) عاماً نظام الكمبيوتر العائد للبنتاغون والآخـر لا يتجاوز عمره السابعة عشر تمكن من اختراق كمبيوترات العديد من المؤسسات الإستراتيجية في اوروبا والولايات المتحـدة ومن بينها الكمبيوترات المتصلة ببرنامج حرب النجوم الذي كان مخطـط لتنفيـذه مـن قبـل الولايـات المتحـدة في حقبـة الحرب الباردة.

أما السمة المميزة الأخرى لهذه الطائفة تبادلهم للمعلومات فيما بينهم وتحديداً التشارك في وسائل الاختراق وآليات نجاحها وإطلاعهم بعضهم البعض على مواطن الـضعف في نظـم الكمبيـوتر والـشبكات، حيـث تجـري عمليـات التبـادل للمعلومات فيما بينهم وبشكل رئيس عن طريق النشرات الإعلامية الإلكترونية ومجموعـات الأخبـار. وفي تطـور حـديث لتنظيم هذه الطائفة نفسها يجري عقد مؤتمرات للمخترقي الكمبيوتر يدعى له الخبراء من بينهم للتـشاور حـول وسـائل الاختراق ووسائل تنظيم عملهم فيما بينهم، وبالرغم من أن الخطورة في هـؤلاء تكمـن بمثـابرتهم عـلى أنـشطة الاخـتراق وتطوير معارفهم التقنية، وبالرغم من توفر فرصة استغلال هؤلاء من قبل مـنظمات وهيئـات إجراميـة تـسعى للكـسب المادي، فإنه ومن ناحية أخرى ساهم العديد من هؤلاء المخترقين في تطوير نظم الأمن في عشرات المؤسسات في القطاعين الخاص والعام، حتى أن العديد من الجهـات تـستعين بخـبراتهم في أحيـان كثـيرة في فحـص وتـدقيق مـستوى أمـن نظـم الكمبيوتر والمعلومات(٨).

هل الهاكرز مسالمون أم مجرمون؟

عندما يشعر بعض الأفراد بأنهم مبعدون من قبل المجتمع فإن ذلـك الـشعور يجعلهـم أحيانـاً يرتكبـون أفعـالاً قـد تكون أحياناً أفعال إجرامية بحق أنفسهم، وبحق المجتمع كذلك، ولذلك يتطلب الأمر هنا فك حالة الالتبـاس والغمـوض والخلط بين مجرمي تكنولوجيا المعلومات وبين الهاكرز، عادة مـا يـشعر الأشـخاص الـذي يكتبـون بـرامج الفيروسـات أو الهاكرز بأنهم مستبعدين من المجتمع. على الرغم أنهم عادة ما يتمتعون بالذكاء، إلا أنهم غالباً لا يرغبـون في أن تكـون لهم وظائف دائمة. وفي بعض الأحيان، يرغب هؤلاء الأشخاص في أن تصيبهم الشهرة، أو يدرك

الآخرون قدراتهم العقلية ومهاراتهم على الأقل، ولكن في الغالب لا يكون المال هو دافعهم الأساسي، فهم غالباً ما يحتجون ويطلبون أن تكون المعلومات مجانية. ولكن لا يستطيع أي شخص الحصول على متطلبات المعيشة بلا مقابل. فإذا قام شخص ما بإنتاج معلومات مفيدة، يصبح من حقه الحصول في مقابلة جهوده على ما يكفي من المال لمواجهة نفقات معيشته. كما أن نظرية الهاكرز التي تطالب بفكرة المعلومات المجانية تتجاهل الكم الهائل من العمل الذي يسبق حصول الهاكرز على إمكانية الوصول إلى الإنترنت وأجهزة الكمبيوتر.

يعد الهاركز في أغلب الأحوال، نسخة ذكية وعقلانية من المراهقين الذين يخربون الحوائط وغيرها من الأشياء عن طريق الكتابة عليها باستخدام الألوان. وبما أنهم يشعرون بالضعف، فكل ما يمكنهم فعله على الأقل هو اقتحام شبكة الكمبيوتر الخاصة بأحد المستخدمين وترك بصماتهم عليها ومن ثم يجعلون الآخرين يدركون وجودهم. فالحياة الاجتماعية لهؤلاء الأشخاص لا تمنحهم ما يكفي من انتباه الآخرين، لذلك فهم يجبرون الآخرين على إدراك وجودهم.

لكن من المستحيل بالطبع تطبيق هذا التصور على المجموعة بأكملها، حيث لا يشعر بالضرورة كل الهاكرز بعدم أهميتهم الاجتماعية أو بالانطواء على الرغم من نبوغهم. فمن المحتمل أن يكون بعضهم أشخاص عاديين لهم جاذبيتهم وأهميتهم في المجتمع.

أخيراً، عندما يكبر هؤلاء الهاكرز، ينضم الموهوبين منهم إلى الجبهة الأخرى حيث ينتهي بهم الحال بالعمل لحساب الحكومية أو المصالح التجارية التي سبق لهم رفضها وسخطها.

قام أشهر الهاكرز (Kevin mitenik) على سبيل المثال، بالمثول أمام الكونجرس ليدلي بشهادته. كذلك قامت بعض الشركات الكبرى بتعيين العديد من الهاكرز كمتخصصي أمن بالإضافة إلى ذلك اتحد بعض الهاكرز وقاموا بتكوين شركات للإستشارات الأمنية.

يتم التفريق من حين لآخر، بين الهاكرز الذي يتسلل إلى نظم الكمبيوتر بغرض إشباع فضوله بالإطلاع على معلومات الآخرين والهاكرز الحقيقي الذي يتسلسل إلى نظم الكمبيوتر بغرض التدمير والتخريب. على الرغم من وجود بعض الأسباب المعرضة وراء هذا التفريق، إلا أنه يشتمل على شيء من الحقيقة. ويقال: إن الهاكرز الذي يكون غرضه الأساسي هو التسلسل إلى نظم الكمبيوتر ينصب اهتمامه الرئيس على أساليب فك التشفير وذلك لكي يرى ما إذا كان يمكنه اختراق نظم الأمان، أو لكي يتعرف على المزيد عن الشبكات والنظم وينصب اهتمام هذا النوع الهاكرز على الناحية الأكاديمية، ولكنه لا يقوم بالتخريب على الإطلاق ويشبه الهاكرز من

هذا النوع مراقبي الطيور، الذين يراقبون فقط كي يتمكنون من رؤية كل شيء دون إلحاق ضرر حقيقي بالطيور أو الهدف الذي يراقبونه.

ينطبق هذا التعريف على العديدين، حتى أنه ينطبق على أي شخص محب للتعليم والمعرفة، ولكن وسائل الإعلام العامة يتجاهلون هذا الفرق. والحق يقال: إن بعض سلوكيات الهاكرز تتراوح ما بين السلوك الجيد والسلوك السيء. (وهذا جواب لسؤال البدء)، كذلك اتجه هاكرز (نظم التليفون) للعمل في شركات التليفون مقابل ما يكفي من المال. وبالطبع كان عملهم هو الحفاظ على نظم الأمان وقد ساعد هؤلاء الهاكرز شركات التليفون على منع هجمات (هاكرز نظم التليفون) وعلى تدعيم نظم هذه الشركات لتجنب وقوع المشكلات في المستقبل.

تشتمل وبالمثل أساليب تخريب أجهزة الكمبيوتر أو الإنترنت على العديد من الأمثلة لأشخاص بدءوا أشراراً ولكن انتهى بهم الحال بالعمل لصالح الجبهة الأخرى كمستشاري نظم أمان، حيث اقلع هؤلاء الأشخاص عن أساليبهم الملتوية وقبلوا بالتأمين المالي الذي تزودهم به وظائفهم الجديدة.(٩).

هل هناك فرق بين الهاكرز المتطفل والهاكرز المتسلل؟

هناك فئات ثانوية داخل مجتمع الهاكرز، ويتم تحديد كل فئة من هذه الفئات عن طريق تحديد كيفية تطبيق كل فئة لأخلاقيات الهاكرز غير الرسمية والمتفق عليها فيما بينهم. ويقوم هاكرز الكمبيوتر (حتى المبتدئين الذين يطلق عليهم مجتمع الهاكرز اسم صغار الهاكرز) باستكشاف واختراق نظم التشغيل وغيرها من شفرات الكمبيوتر التي من المفترض أن تكون مؤمنة، ولكنهم لا يدّمرون أن يسرقوا الأموال أو المعلومات. فالغرض الأساسي الذي يسعى هذا النوع من الهاكرز إلى تحقيقه هو محاولة التأكد من حرية المعلومات عن طريق جعل إمكانية الوصول لأجهزة الكمبيوتر والمعلومات عملية غير مقيدة.

بات واضحاً أن هناك خطر دائم يحيط بخصوصية مستخدمي الكمبيوتر وبالتالي بحرياتهم والذي يفرضه عليهم تجميع الحكومة المستمر للبيانات. ومما يؤيد إدعاءات مجتمع الهاكرز أن الغرض من اقتحامهم ودراستهم محتويات قواعد البيانات الخاصة بالهيئات الحكومية والشركات هو خلق نوع من توازن القوى في عصر المعلومات.

يهدف الهاكرز بأنشطتهم إلى تحقيق العديد من الفضائل والمصالح العلمية، فبإبطائهم مواقع التجارة الإلكترونية (ومن خلال هجمات denial of service، التي يقومون فيها بتحميل عبء كبير على المكالمات الواردة بشكل مستمر وبسرعة)، يجبر الهاكرز تلك المواقع على تطبيق

المزيد من نظم الحماية ضد الأخطار المماثلة. وباقتحامهم للشبكات المفترض أن تكون مؤمنة، فإنهم يجبرونها على تطبيق نظم الأمان المحكمة. وبالطبع، يمكن تطبيق هذا المنطق العقلاني على أي من سلوكياتهم السيئة - على الرغم مما يشتمل عليه ذلك من خطأ. وعادة ما يكون دافع الهاكرز هو الفضول، الذي ربما يكون ممزوجاً بالرغبة في المعرفة. أما الإدعاء بأن جهود هؤلاء الهاكرز تعتبر دعوة للإصلاح ما هو إلا مجرد إدعاء ليس له أساس من الصحة.

فوق هذا وذاك، يجب إتباع المنطق الذي يحكم مجتمع الهاكرز ويجب استيعاب الطريقة التي يحبون النظر بها إلى أنفسهم، والتي يمكن استنتاجها من لغتهم والفوارق التي يرغبون في وضعها فيما بينهم.

يمكن تعريف الهاكرز الذين يكون دافعهم الأساسي هو التطفل على أنهم هاكرز المستقبل والذين يحصرون أنفسهم في نطاق استكشاف وفحص النظم بدون محاولة القيام بأية عمليات تخريب كبيرة (اختراقات أمنية). أما الهاكرز الذين يكون دافعهم الأساسي هو التخريب فهم هؤلاء الذين يتعدون تلك الحدود وينصب اهتمامهم على سرقة المعلومات متسببين في إحداث أنواع متعددة من الدمار (محو محركات الأقراص الصلبة)، وفي بعض الأحيان يتسببون في تدمير نظم بأكملها.

عادة يعتبر هذا النوع الأخير نفسه أفضل من الأنواع الأخرى من الهاكرز؛ وذلك لأن أفراد هذا النوع غالباً ما يكونوا غير معقدين ويسعون دائماً للتدمير. وعلى الرغم من مهارة بعضهم، إلا أن العديد منهم لا يفكر بطريقة معّقدة حتى أن تفكيرهم يبدو كتفكير الأطفال في بعض الأحيان وغالبا يستبدل هؤلاء الهاكرز الإصرار القوي ومجموعة الخدع المتكررة، التي تستفيد من نقاط الضعف الموجودة في نظام الأمان، بالابتكار والتعقيد التكنولوجي. ويستخدم بعضهم الآخر البرامج التي تؤدي إلى إحداث التلف والدمار في أنظمة الكمبيوتر والتي يقومون بتنزيلها واستخدامها، ولكن بدون أن يتمكنوا من فهمها.

لا يتسم العديد من هؤلاء الهاكرز بالمهارة، فهم مجرد مجموعة من المرضى والمنحرفين. وعلى العموم، توجد علاقة وثيقة بينهم وبين غيرهم من المجموعات الصغيرة السرية الغاضبة، التي تكون في منآى عن مجتمع التبادل الحر والذكي للمعلومات الذي يدعمه الهاكرز الآخرون. ويتضح هذا الفرق طياً في مجتمع الهاكرز المتسللين على الرغم من ذلك، عادة ما يفقد الفرق بين هذين النوعين من الهاكرز- هاكرز بدافع التخريب وهاكرز بدافع التسلل - في وسائل الإعلام

ومن خلال استخدام العامة. وبالطبع، دائماً ما يدعي الهاكرز المخربين بأن هدفهم هو مجرد التسلل.

يتضح على الرغم من ذلك، من التحليل الأخير أن عمليات التسلل التقليدية تعادل عمليات اقتحام المنازل والتجـول فيها الإطلاع على محتوياتها. ولكن من الواضح أنه لا يعادل أية أفعال شريرة مثل السرقة أو شن الحرائـق - عـلى الـرغم من أنه بالنسبة للعديدين تعتبر عملية الاقتحام البسيطة خطأ جسيماً.(١٠).

٢- مجرمو الكمبيوتر المحترفون:

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطـيط للأنـشطة التـي ترتكب من قبل أفرادها، ولذلك فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم اعتداءاتهم بالأساس إلى تحقيق الكسب المـادي لهـم أو للجهـات التي كلفتهم وسخرتهم لارتكاب جرائم الكمبيوتر، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبـير عـن موقف فكري أو نظري أو فلسفي.

يتم تصنيف أفراد هذه الطائفة إلى مجموعات متعددة أما تبعاً لتخصصهم بنوع معين من الجرائم أو تبعاً للوسـيلة المتبعة من قبلهم في ارتكاب الجرائم، فمثلاً نجد طائفة محترفي التجسس الصناعي وهم أولئك الذين يوجهون أنـشطتهم إلى اختراق نظم الكمبيوتر العائدة للشركات الصناعية ومشاريع الأعمال بقصد الإستيلاء على الأسرار الـصناعية والتجاريـة أما لحساب أعمال يقومون بها بذاتهم أو في الغالب لحـساب منافـسين آخـرين في الـسوق وأحيانـاً لحـساب مجموعـات القرصنة الدولية.

نجد على سبيل المثال، طائفة مجرمي الاحتيال والتزوير، وهؤلاء هـم الطائفة التي تكون أغراضها متجهة إلى تحقيـق كسب مادي والاستيلاء على أموال الآخرين، وضمن هذه الطائفة أيـضاً ثمـة تـصنيفات عديـدة فمـنهم محتـالوا شـبكات الهاتف، محتالوا الانترنت وغير ذلك، وحتـى في الطائفـة الفرعيـة، قـد تتـوفر تخصـصات لبعـضهم كـأن يوجـه الـشخص أنشطته الاحتيالية إلى قطاع مزادات البضاعة والمنتجات على الإنترنت أو في ميدان الاستيلاء على أرقـام بطاقـات الائـتمان والاتجار بها.

أضف إلى ذلك، وإلى جانب المعرفة التقنية المميزة والتنظيم العالمي والتخطيط للأنشطة المنوي ارتكابها، فـإن أفـراد هذه الطائفة يتسمون بالتكتم خلافاً للطائفة الأولى فلا يتبادلون المعلومات

بشأن أنشطتهم، بل يطورون معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لإرتكاب جرائمهم، وحول الأعمال الغالبة على هذه الطائفة فإن الدراسات تشير إلى أنهم من الشباب الأكبر سناً من الطائفة الأولى وأن معظمهم تترواح أعمارهم ما بين (٢٥-٤٠) عام.

٣- الحاقدون:

هذه الطائفة يغلب عليها عدم توفر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون أما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو على علاقة بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم، ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يشقى الواحد منهم في الوصول إلى كافة عناصر المعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه، وتغلب على أنشطتهم من التقنية استخدام تقنيات زراعة الفايروسات والبرامج الضارة وتخريب النظام أو إتلاف كل أو بعض معطيات ، أو نشاط إنكار الخدمة وتعطيل النظام أو الموقع المستهدف إن كان من مواقع الإنترنت.

ليس هناك ضوابط محددة بشأن أعمارهم، كما أنه لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة، ولا يفاخرون بأنشطتهم، بل يعمدون إلى إخفائها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد في ذلك، وبالرغم من أن سمات هذه الطائفة تضعها من حيث الخطورة في مؤخرة الطوائف المتقدمة، إذ هم أقل خطورة من غيرهم من مجرمي التقنية، ولكن ذلك لا يمنع أن تكون الأضرار التي نجمت عن أنشطة بعضهم جسيمة ألحقت خسائر فادحة بالمؤسسات المستهدفة.

٤- طائفة صغار السن:

فئة صغار السن، أو كما يسميهم البعض (صغار نوابع المعلوماتية)، ويصفهم بأنهم "الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية"، فإن من بينهم في الحقيقة ، فئة لم تزل دون سن الأهلية مولعين بالحوسبة والاتصال. وقد تعددت أوصافهم في الدراسات الاستطلاعية والمسحية، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح (المتلعثمين)، الدال، حسب تعبير الأستاذ توم فورستر ، على "الصغار المتحمسين للحاسوب، بشعور من البهجة، دافعهم التحدي

لكسر الرموز السرية لتركيبات الحاسوب"، ويسميهم البعض كذلك بمجانين (معدلات ومعدلات عكسية)، بالاستناد إلى كثرة استخدامهم لتقنية المعدل والمعدل العكسي (الموديم)، الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم، ويثير مجرمو الحوسبة من هذه الطائفة جدلاً واسعاً، ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، على الأقل مواصلتها العبث بالحواسيب، ظهرت دراسات ومؤلفات تدافع عن هذه الفئة، لتخرجها من دائرة الإجرام إلى دائرة العبث، وأحياناً البطولة. من هذه المؤلفات على سبيل المثال، كتاب (خارج نطاق الدائرة الداخلية. كيف تعملها؟) لمؤلفه الأمريكي "لبيل لاندريت)، وكتاب (الدليل الجديد للمتلعثمين) لمؤلفه "هوجو كورن" في المملكة المتحدة، وكتاب (المتلعثمون - أبطال ثورة الحاسوب)، لمؤلفه "ستيفن ليفي").

من الأمثلة الشهيرة لجرائم الحاسوب التي ارتكبت من هذه الفئة، العصابة الشهيرة التي أطلق عليها (عصابة ٤١٤)، والتي نسب إليها ارتكاب ستون فعل تعد في الولايات المتحدة الأمريكية على ذاكرات الحواسيب، نجم عنها أضرار كبيرة لحقت بالمنشآت العامة والخاصة. وكذلك، تلاميذ المدرسة الثانوية في ولاية (منهاتن) الذين استخدموا في عام (١٩٨٠) طرفيات غرف الدرس للدخول إلى شبكة اتصالات وبيانات العديد من المستخدمين ودمروا ملفات زبائن الشركة الرئيسة في هذه العملية. كما سبب متلعمو ألمانيا الغربية الصغار في عام (١٩٨٢) فوضى شاملة، عندما دخلوا إلى شبكة (الفيديوتكس) ونجح بعض المتلعثمون الفرنسيون في إيجاد مدخل إلى الملفات السرية لبرنامج ذري فرنسي.

يمكن رد الاتجاهات التقديرية لطبيعة هذه الفئة، وسمات أفرادها، ومدى خطورتهم في نطاق ظاهرة جرائم الحاسوب إلى ثلاثة اتجاهات:

الأول: اتجاه لا يرى إصباغ أية صفة جرمية على هذه الفئة، أو على الأفعال التي تقوم بها، ولا يرى وجوب تصنيفهم ضمن الطوائف الإجرامية لمجرمي الحواسيب، استنتاجاً إلى أن صغار السن (المتلعثمين) "لديهم ببساطة ميل للمغامرة والتحدي، والرغبة في الاكتشاف، ونادراً ما تكون أهدافه، أفعالهم المحظورة غير شرعية، واستناداً إلى أنهم لا يدركون ولا يقدرون مطلقاً النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشآة أو شركة تجارية.

الثاني: الإتجاه الذي يحتفي بهذه الفئة ويناصرها يعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصفهم بالأخيار وأحياناً بالأبطال الشعبيين، ويتمادى هذا الاتجاه في تقدير لهذه

الفئة بالمطالبة بمكافئتهم بوصفهم لا يسببون ضرراً للنظام ، ولا يقومون بأعمال احتيال، وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات. ومثل هذا الرأي قاله به أحد أشهر المدافعين عن الهاكرز الصغار، "هيوجوكرون ول"، تم منع مؤلفه المذكور من قبل مركز بوليس مدينة لندن الكبرى (سكوتلاندرياد)، غير أن هذا المنع كان له أثر في توسيع دائرة انتشار هذا الكتاب وتحقيق نسبة عالية جداً من المبيعات.

يتمادى الإعلامي (ستيفن ليف) في الإحتفال بهذه الفئة ، واصفاً إياها بأبطال ثورة الحاسوب متحمساً لهذا الوصف إلى درجة إطلاقه عنواناً على مؤلفه الخاص بهذه الظاهرة، لا لموقف معاد من التقنية، بل لأنه يرى في دوافعهم الخيّرة لا الشريرة، المواجهة لمالكي الأموال لا المحتاجين، ما ينهض بوصفهم بالأبطال الشعبيين.

الثالث: اتجاه يرى أن مرتكبي جرائم الحاسوب من هذه الطائفة، يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييز استناداً إلى أن تحديد الحد الفاصل بين العبث في الحواسيب وبين الجريمة أمر عسير من جهة، ودونما أثر على وصف الفعل قانوناً من جهة أخرى، واستناداً إلى أن خطورة أفعالهم تتميز بانتهاك الأنظمة واختراق الحواسيب وتجاوز إجراءات الأمن، والتي تعد بحق من أكثر جرائم الحاسوب تعقيداً من الوجهة التقنية، عوضاً عن مخاطرها المدمرة كما عرضناه سابقاً.

يدعم صحة هذا الاتجاه، التخوفات التي يثيرها أصحاب الاتجاه الأول ذاتهم، إذ يخشون من الخطر الذي يواجه هذه الطائفة، والمتمثل باحتمال الانزلاق من مجرد هاو صغير لاقتراف الأفعال غير المشروعة، إلى محترف لأعمال السلب ، هذا إلى جانب خطر آخر أعظم، يتمثل في احتضان منظمات الإجرام ومجرمين غارقين في الإجرام لهؤلاء الشباب، محترفو جرائم الحاسوب.

٥- المجرمون البالغون: محترفو الإجرام.

إن مرتكبي جرائم الحاسوب عموماً، ينتمون وفق الدراسات المسحية إلى فئة عمرية تتراوح بين (٢٥-٢٤) عاماً، وبالتالي، يمتاز مرتكبو هذه الجرائم بصفات الشباب العمرية والاجتماعية، وإذا استثنينا صغار السن من بينهم، الذين تكون أعمارهم دون الحد الأدنى المشار إليه أعلاه، كما رأينا فيما سلف، فإن لمجرمي الحاسوب سمات عامة، يتحقق بعضها لدرجة أقل في صغار السن وهذه السمات إضافة لما أوردناه في الطوائف المتقدمة تتمثل بما يلي:

أولاً: الصفات الشخصية والتخصص والكفاءة:

الجامع بين محترفي جرائم الحاسوب، تمتعهم بقدرة عالية من الذكاء، وإلمام جدي بالتقنية العالية، واكتسابهم معارف عملية وعلمية، وانتمائهم إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية، وهذه السمات تتشابه مع سمات مجرمي ذوي الياقات البيضاء، أما فيما يتعلق بكفاءة مجرمي الحاسوب، فإن الدراسات القليلة المتوفرة تشير إلى تمتعهم بكفاءة عالية، إلى درجة اعتبارهم مستخدمين مثاليين من قبل الجهات العاملين لديها، وممن يسمون بالنشاط الواسع والإنتاجية الفاعلة.

ثانياً: من حيث السيكولوجية:

إن الدراسات القليلة للجوانب السيكولوجية لمجرمي الحاسوب، أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية وبلا مشروعة الأفعال التي يقترفونها، كذلك بعدم استحقاقهم للعقاب عن هذه الأفعال، فحدود الشر والخير متداخلة لدى هذه الفئة، وتغيب في دواخلهم مشاعر الإحساس بالذنب، وهذه المشاعر في الحقيقة تبدو متعارضة مع ما تظهره الدراسات من خشية مرتكبي جرائم الحاسوب من اكتشافهم وافتضاح أمرهم، ولكن هذه الرهبة والخشية يفسرها انتماؤهم في الأعم الأغلب إلى فئة اجتماعية متعلمة ومثقفة.(١١).

٢- ما الدوافع وراء ارتكاب جرائم تكنولوجيا المعلومات؟

مما لا شك فيه أن وراء كل فعل سواء كان يحمل في طياته جانب الخير أم الشر إلا وخلفه دافع أو غرض أو غاية، ولهذا ولذاك فإن، الدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالاته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلاً فقهياً وقضائياً واسعاً، ذلك أن "القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي"، وأن الباعث " لا أثر له في وجود القصر الجنائي" وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية. فالباعث (المدافع) هو " العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء أو الانتقام"، وهو إذن قوة نفسية تدفع الإرادة إلى الإتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو " يختلف من جريمة إلى أخرى، تبعاً لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر.

أما الغرض، "فهو الهدف الفوري المباشر للسلوك الإجرامي ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات"، وأما الغاية، " فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام أو سلب مال المجني عليه في جريمة القتل".

إن الباعث والغاية في الأصل، ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين، علم الجاني بعناصر الجريمة، واتجاه إرادته إلى تحقيق هذه العناصر أو إلى قبولها، ولا تأثير للباعث أو الغاية "على قيام الجريمة أو العقاب عليها، فالجريمة تقوم بتحقق عناصرها سواء كان الباعث نبيلاً أو رذيلاً وسواء كانت الغاية شريفة أو دزريئه، وإذا كانت القاعدة أن الباعث أو الغاية لا أثر لهما على قيام الجريمة، فإن القانون يصيغ عليهما في بعض الأحيان أهمية قانونية خاصة".

بالنسبة لجرائم الكمبيوتر والإنترنت، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الإعتداء المختلفة المنضوية تحت هذا المفهوم، ويمكننا من خلال الحالات التطبيقية تبين الدوافع الرئيسة الآتية:

أولاً: السعي إلى تحقيق الكسب المالي:

يعد هذا الدافع (والذي يمثل في الحقيقة غاية الفاعل) من بين أكثر الدوافع تحريكاً للجناة لاقتراف جرائم الحاسوب، ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها، لا سيما غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع.

منذ بدايات الظاهرة، فإن الدراسات أشارت إلى أن المحرك الرئيس لأنشطة احتيال الكمبيوتر، وفيما بعد احتيال الإنترنت، هو تحقيق الكسب المالي، ففي دراسة قيمة عرض لها الفقيه (PARKER) يظهر أن (٤٣%) من حالات الغش المرتبط بالحاسوب المعلن عنها قد بوشرت من أجل اختلاس المال، وهي النسبة الأعلى من بين النسب التي حققتها جرائم أخرى في هذه الدراسة (٣٢%) سرقة معلومات، ١٩% أفعال إتلاف، ١٥% سرقة وقت الحاسوب (الآلة) لأغراض شخصية).

إذا ما انتقلنا للدراسات الحديثة، فسنجد أن هذا الدافع يسود على غيره ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية. وفي مقدمة هذه الدراسات المسحية والتقارير الإحصائية الدراسات والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية، (NFIC).

ثانياً: الانتقام من رب العمل وإلحاق الضرر به:

لقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات عديدة، مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من المنشأة أو رب العمل، وسنجد في معرض تناولنا لأنواع جرائم تكنولوجيا المعلومات، سنجد أمثلة عديدة، كان دافع الجناة فيها إشباع الرغبة بالانتقام، وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيس والتكنيك الغالبة للفئة التي تمثل الأحقاد على رب العمل المحرك لارتكاب الجريمة.

ثالثاً: الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية:

يرى بعضهم "أن الدافع إلى ارتكاب الجرائم في الطائفة الأولى (جرائم الحاسوب) يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح"، ومع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها، إذ يظهر في قهر النظام إلا أن الدافع الأخير، يتجسد في نسبة معتبرة من جرائم الحاسوب لاسيما ما يعرف بأنشطة الـ (hackers) المتطفلين الدخيلين على النظام والمتجسدة في جرائم التوصل مع أنظمة الحاسب- تحديداً عن بعد - والاستخدام غير المصرح به لنظام الحاسوب، واختراق مواقع الانترنت.

يميل مرتكبو هذه الجرائم إلى تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم (شغف الآلة) يحاولوا إيجاد، وغالباً ما يجدون، الوسيلة إلى تحطيمها (والأصوب التفوق عليها). ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي جرائم الحاسوب، الذين يمضون وقتاً طويلاً أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات، ولإظهار تفوقهم على وسائل التقنية، ونكتفي بالقول هنا: إن هذا الدافع هو أكثر الدوافع التي يجري استغلالها من قبل المنظمات الجرمية (مجموعات الجريمة المنظمة) لجهة استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.

رابعاً: دوافع أخرى:

كانت تلك أبرز دوافع ارتكاب جرائم تكنولوجيا المعلومات، لكنها ليست كل الدوافع، فمحرك أنشطة الإرهاب الإلكتروني، وحروب المعلومات، الدوافع السياسية والأيديولوجية، في

حين أن أنشطة الإستيلاء على الأسرار التجارية تحركها دوافع المنافسة، والفعل الواحد قد يعكس دوافع متعددة خاصة ما إذا اشترك فيه أكثر من شخص انطلق كل منهم من دوافع خاصة تختلف عن غيره، ويمكننا أخيراً أن نضع التصور - الرياضي- الآتي لدوافع بعض الهجمات الشائعة في حقل جرائم الكمبيوتر والإنترنت.

أ- حروب المعلومات والإرهاب والإلكتروني = دوافع سياسية أو فكرية.

ب- إنكار الخدمة للمواقع التجارية والخدمية = التحدي وقهر النظام + أفعال ثأرية وأحقاد موظفين + التنافسية بأنشطة غير مشروعة.

ج- احتيال الكمبيوتر واحتيال الإنترنت = استيلاء على المال أو المنافع وتحقيق الربح.

د- الاستيلاء على المعلومات = التنافسية+ ابتزاز الأفراد وتحقيق المكاسب + المنافع+ الأفعال الثارية+ الأعداد للهجمات ذات الدوافع المالية.

هـ- إتلاف المعطيات وتخريب الأنظمة = الأحقاد والدوافع الثارية +إخفاء الأنشطة الجرمية الأخرى+ التنافسية غير المشروعة+ التحدي وتحديداً بالنسبة لبرامج الفيروسات.(١٢).

٣- الظروف البيئية لارتكاب جرائم تكنولوجيا المعلومات:

ربما يتساءل أحدهم عن أهم الظروف التي تتيح للمجرم ارتكاب جريمته ولعل السؤال الأبرز هنا مفاده: هل هناك ظروف معينة فعلاً لارتكاب جرائم تكنولوجيا المعلومات؟ بكل تأكيد تشير وتؤكد مصادر المعلومات والأدلة التاريخية بأنه ما من جريمة حدثت أو تحدث إلاّ وقد تهيأت لها ظروف معينة، وكذلك الحال ينطبق على جرائم تكنولوجيا المعلومات، إذ يجب أن تتوفر الظروف الملائمة حتى يمكن القيام بجريمة بالكمبيوتر أو الإنترنت، ولذلك سنعرض فيما يلي أنسب الظروف التي تسمح للمتلاعب وتهيء له المناخ الملائم لتنفيذ مخططاته الجرامية:

١- عندما تتكامل كافة أجزاء نظام المعلومات الإلكتروني بشكل يسمح للمتآمر أن يدبر تلاعبه بسهولة، حيث في استطاعته إدخال تعديل بسيط في أحد برامج النظام الذي قد تترتب عليه تحريف المعاملات المالية. وفي بعض الأحيان، إصدار شيكات ومخزون سلعي.

٢- عندما تكون العلاقة سيئة للغاية بين الرئيس والمرؤوسين لا سيما عندما تصل إلى حد وجود استياء عام في محيط العمل.

٣- عندما لا تفصل اختصاصات الوظائف لا سيما تلك التي تتطلب درجة عالية من الأمانة وعدم الغش. وبقول آخر عندما يعطي الموظفون مسؤوليات واسعة دون الإشراف على أداء وظائفهم عن قرب.

٤- عندما لا يخضع موظفو الكمبيوتر لإشراف رؤسائهم عند عملهم خلال ساعات خارج الدوام أو أيام العطل الأسبوعية. فعدد كبير من التلاعب تم بواسطة معدي البرامج (بصفة خاصة) أثناء الليل أو أيام العطل، وذلك نظراً لعدم توفر الإشراف اللازم على عمليات هؤلاء الأشخاص.

٥- عندما لا تكون هناك أساليب رقابة فعّالة على برامج تطبيقات الكمبيوتر (برامج الرواتب والأجور، المخزون، المدينون، .... الخ) اللازمة للوقاية ضد أي تلاعب وسوء استخدام لتحقيق مآرب شخصية.

٦- عندما يكون من الصعب اختيار برامج تطبيقات الكمبيوتر أو صعوبة الحصول على مسار مراجعة جيد والذي يمكن بواسطته تتبع مسار العمليات من الألف حتى الياء.

٧- عندما لا يحاسب موظفو مركز الكمبيوتر من استخداماتهم للأجهزة أو البرامج، فيجب مساءلة كافة الموظفين من مشغلي أجهزة ومعدي برامج ومحللي نظم عن استخداماتهم المختلفة للأجهزة والبرامج(١٣).

لقد أشارت الدلائل والحقائق إلى أن وجود أي عدد من هذه العوامل سواء في محيط العمل أو خارجه ستشجع أولئك الأفراد أصحاب النفوس الضعيفة على ارتكاب جرائمهم لتحقيق مآربهم الشخصية بغض النظر التي تقف ورائها.

٤- كيف يتم ارتكاب جرائم تكنولوجيا المعلومات؟

يتم ارتكاب تكنولوجيا المعلومات حسب:

١- مرحلة إدخال البيانات: مرحلة تشغيل البيانات، ومرحلة إخراج البيانات، وبالنسبة لمرحلة إدخال البيانات تحدث الجريمة إذا قام المستخدم بتزوير أو تغيير (فبركة) البيانات، ومثال ذلك: إذا استطاع الجاني الوصول إلى البيانات المتعلقة بفاتورة الهاتف قبل إعدادها بشكلها النهائي من قبل شركة الهاتف وتمكن من حذف بعض المكالمات من الفاتورة قبل إرسالها بالبريد أو أثناء قيام أحد مدخلي البيانات بتغيير الإجراءات أو المستندات الثبوتية لشخص ما أو قام الجاني بتغيير معلومات شخص مشتبه به (محظور).

٢- مرحلة تشغيل البيانات: مرتكبي هذه الجرائم يقومون بتعديل البرامج الجاهزة (soft ware) التي تقوم بتـشغيل البيانات للوصول إلى بيانات نتائج محددة أو مقصودة من قبل الجاني وفي هـذه الحالـة يجـب أن يكـون الجـاني على قدر من الدراية والمعرفة بالنظام (مبرمج أنظمة).

٣- مرحلة إخراج البيانات: أكثر المراحل التي تنتشر فيها جريمة الحاسوب، وتتم في هذه المرحلة سرقة المعلومـات أو البيانات المتعلقة بالرقابة على المخزون في إحدى المصالح، أو إنشاء بعض المعلومات الخاصة بـالإجراءات الأمنيـة الخاضعة للفحص السري لتأمين وضع معين عند موقف عن السلطات العـسكرية أو أي معلومـات بـالوزارات أو بالشركات أو الأفراد.(١٤).

٥- أساليب ارتكاب جرائم تكنولوجيا المعلومات.

لا شك أن هناك أكثر من أسلوب أو طريقة يتم من خلالهـا ارتكـاب جريمـة أو عـدة جـرائم، لاسـيما تلـك المتعلقـة بتكنولوجيا المعلومات، وفيما يلي عدد من الأساليب الشائعة في ارتكاب جرائم تكنولوجيا المعلومات.

١- القنبلة الموقوتـة: (time bomb): ويحـدث أن يـستقبل مـستخدمي الإنترنـت في الوقـت الـراهن رسـائل بريديـة ملغومة بفيروسات مدمرة من مجهولين وتنشيط بمجرد فتح تلك الرسالة. وهي تعليمات غير مرخـصة موضـوعة في برنامج بهدف إجراء عمليات غير مشروعة في وقت محدد مسبقاً أو حين تحقق شروط معينة.

٢- أسلوب تقريب الأرقام: ويستخدم هذا الأسلوب لاستغلال المؤسسات المالية التي تدفع الفائدة.

٣- أسلوب السجق (سلامي): ويستخدم هذا الأسلوب في سرقة المال بمقدار بسيط على مدى فترات طويلة.

٤- أسلوب الباب السحري: وهو تعليمات تعطـي للحاسـب لتـسمح للمـستفيد بتجـاوز قيـود الـتحكم المعتـادة في النظام. وهذه العمليات تعطي للحاسب أثناء تطوير الأنظمة وتحذف في الغالـب قبـل وضـع النظـام في مرحلـة التشغيل النهائي.

٥- البرامج المعدة لأغراض محددة: استخدام برامج النظام الخاصة مثل (سوبر زاب super zap)، الذي تم تطويره في (IBM) لاستخدامه في حالة الطواريء لتجاوز قيود التحكم العادية وتنفيذ عمليات غير مشروعة.

٦- قرصنة البرامج: وتعني النسخ غير المفوض للبرامج.

٧- غش البيانات: ويشمل حذف البيانات، أو تغييرها، أو إضافتها قبل أو بعد أو في أثناء إدخالها في النظام.

٨- تسريب البيانات: وتعني النسخ غير المفوض للبيانات.

٩- التصنت على الاتصالات السلكية واللاسلكية.

١٠- التزوير: ويحدث عندما يستخدم شخص غير مفوض رقم هوية وكلمة السر الخاصة بمستفيد مفوض.

١١- الهواية.

١٢- الخداع الإلكتروني : ويحدث هذا النوع عندما يتصل مخادع آلياً بمستفيد مفوّض ويوهمه بأنه له حق الاستفادة من النظام.(١٥).

٦- أنواع جرائم تكنولوجيا المعلومات:

تقديم:

مما لا شك فيه أن جرائم تكنولوجيا المعلومات باتت تشكل اليوم ظاهرة في المجتمعات الإنسانية، لاسيما مجتمع المعلومات العالمي، ولذلك أصبح المجتمع أمام مسؤولية جديدة وخاصة أولئك المتخصصين في مجال أمن المجتمع من رجال القانون، وعلم الاجتماع وعلم النفس، ورجال الأمن.. الأخ. وباتت المسؤولية الجديدة تملي عليهم معرفة أنواع أو أنماط جرائم تكنولوجيا المعلومات، ومحاولة الوقوف أمام كل جريمة. لقد أصبحت جرائم تكنولوجيا المعلومات تمثل مجموعة من الأنماط الإجرامية التي تتم عبر أنواع تكنولوجيا المعلومات المختلفة سواء تلك المتمثلة بتكنولوجيا التخزين والاسترجاع (الأقراص الصلبة، والأقراص المرنة) أو المتجسدة بتكنولوجيا الاتصالات الحديثة ولاسيما (الإنترنت) ولهذا ولذلك، يتطلب الأمر كشف النقاب عن أنواع جرائم تكنولوجيا المعلومات من خلال تسليط الضوء على أهم أنواعها، وفيما يلي تلك الأنواع:

١- جريمة الإرهاب الإلكتروني:

يقصد بالإرهاب لغوياً هو إرهاب المدنيين والاعتداء على أرواح وممتلكات الآمنين، من أجل بلوغ مطالب شخصية. فالإرهابي المجرم هو ذاك الشخص الذي يفتقر إلى قضية عادلة يدافع عنها وإنسان تعوزه الأخلاق الإنسانية والمسؤولية الاجتماعية، فيرتكب اعتداءات على الآخرين.(١٦).

أما المعني الاصطلاحي لمفهوم الإرهاب، فو متأتي من الرهبة أي الخوف أو هو التخويف وإشاعة عدم الاطمئنان وبث الرعب والفزع وغايته إيجاد عدم الاستقرار بين الناس في المجتمع

لتحقيق أهداف معينة، فالإرهاب هو العنف المخيف، كما أنه العنف الذي يمارس الإنسان وحقوقه الأساسية أيا كان مصدره أو القائم به ويمكن وصف الإرهاب بأنه العنف السياسي أي الرعب والخوف الذي تقوم به جماعة أو أفراد أو شخص أو دولة أو منظمة لتحقيق أغراض أو أهداف معينة من وراء ذلك.

كذلك هو ظاهرة من ظواهر الاضطراب السياسي في العصر الحديث، وعلى الرغم من أن الإرهاب، أي العنف السياسي ضد الشعب. ولابد من القول هنا: إن مفهوم الإرهاب هو مفهوم نسبي متطور يختلف من مكان إلى آخر ومن فرد إلى آخر ومن عقيدة أو فكر إلى آخر، ولهذا فمن الصعب أن نقر أو نقول بوجود مفهوم واحد للإرهاب أو للجريمة السياسية أو للعنف السياسي يمكن أن يقبل به الجميع.(١٧).

أما الآن ومع التقدم التقني (MODERN IECHNIQES) ومع تقدم وسائل الاتصال (COMMUNICATION TECHNIQUES)، الذي نعيشه ونكاد نلمسه فقد تغيرت وتطورت تلك الأساليب، "Systems"، الذي يحاول الإرهابيين منها الوصول إلى أهدافهم، فقد أصبح الإرهاب الإلكتروني هو السائد حالياً وأصبح اقتحام المواقع "STORMINGSITES)، وتدميرها وتغير محتوياتها والدخول على الشبكات أو العبث بمحتوياتها بإزالتها أو الإستيلاء عليها أو الدخول على شبكات الطاقة أو شبكات الاتصالات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً هو أسلوب الإرهاب (SYSTEMS of TERRORISING) حالياً في محاولة الوصول إلى أغراضهم.(١٨).

أضف على ذلك ، يمكن القول: إن قاموس العصر الحديث بات يزخر بالعديد من مصطلحات العنف المعلوماتي، نذكر منها على سبيل المثال لا الحصر الآتي:

١. العنف الرمزي.

٢. الاستغلال المعلوماتي.

٣. الفجوة الرقمية.

٤. احتلال الفضاء المعلوماتي.

٥. التجويع المعرفي.

٦. ضراوة أجهزة الإعلام.

٧. العصف بالعقول.

٨. تزييف العقول عن بُعد.

٩. الإمبريالية الرقمية.

١٠. القمع الأيديولوجي.

بشكل عام، يمارس العنف المعلوماتي أو الإرهاب الإلكتروني من خلال ما يمكن أن نطلق عليه (القوى الرمزية اللينة)، (Soft Powers) التي تختلف جوهرياً عن القوى التقليدية الصلبة (hard Powers)، فهي تعمل بالجذب لا بالضغط، وبالترغيب لا بالترهيب، وتستخدم لغة تخاطب العقول والقلوب، من أجل اكتساب الآراء لا كسب الأرض، ومن أجل انتزاع الإرادة الجماعية لا نزع السلاح والملكية، ومن أجل فرض المواقف وزرع الآراء بدلاً من فرض الحصار وزراعة الألغام. ونستطرد في حديث الفوارق بين القوى اللينة والقوى الصلبة لنشير إلى كيف أصبح توسيع نطاق الإعلام في مقام نشر القوات، وأصبحت الأجندة في مقام التكتيك، والهوائيات والفضائيات في مقام ترسانات الأسلحة ومنصات الصواريخ، وهكذا أصبح التلفاز، وغيره من وسائل الإعلام آلة حرب كأسلحة لا بد أن نتصدى لها بالدروع والمتاريس. ألم نسمع عن القمر الصناعي للبث التلفازي الذي كانت الولايات المتحدة (تحت إدارة جورج بوش الاب) تنوي إطلاقه بهدف إسقاط حكم كاسترو المناهض لها في كوبا؟

تختلف القوى الليّنة عن القوى الصلبة، من حث أسلوب الممارسة، في أمور عدة أساسية، من أهمها: القدرة الهائلة على المناورة بالقوى اللينة زمنياً وجغرافياً، وكون القوى الصلبة لا تستخدم إلا في حالات الضرورة القصوى في حين تمارس القوى اللينة بصورة مستمرة ودائمة.

أما في وقت الأزمات والحروب والصراعات، توضع القوى الرمزية اللينة في خدمة القوى التقليدية الأخرى، ويشهد التاريخ، من الحرب الصليبية إلى الحروب الأهلية بين قبائل الشعوب الإفريقية والآسيوية، كيف وقفت القوى الرمزية إلى جانب القوى العسكرية والسياسية، ويكفي أمثلة هنا، ما قامت به إذاعة ألمانيا النازية في أثناء الحرب العالمية، وكذلك الدور الذي تلعبه وكالة المخابرات المركزية في كواليس السياسة الأمريكية. لكن أكثر الأمثلة مرارة وبشاعة في إساءة استخدام القوى الرمزية هو ما فعلته إذاعة "ميل كولينز" في رواندا بإشعالها نيران الفتنة القبلية بأهل هذا البلد الإفريقي بلا ذنب لهم ولا جريرة، فقد فاق ما حصده هذا البوق الإعلامي اللاأخلاقي من ضحايا قبائل التوتسي ما فعلته القنبلة الذرية بأهل هيروشيما ونجازاكي.(١٩).

إزاء ما تقدم، يمكن أن نقول: إن ظاهرة الإرهاب المعلوماتي: قادته بل وساعدت على انتشار تكنولوجيا المعلومات. إن الإرهابي الذي يمارس نشاطه في ظل مجتمع ليبرالي، يعلم أن أعماله الإرهابية سوف يذيعها التلفاز في الحال، وكذلك الراديو والصحافة، وأن صور الهجوم والعنف يمكن أن تُذاع حول العالم من خلال الأقمار الصناعية. ويذهب بعضهم إلى أن الإرهابيين والقائمين. بالتغطية الإخبارية التليفزيونية يتعاونون في تصعيد الرعب ومعدلات المشاهد. ورغم أنه لا يزال يوجد إرهاب دون تغطية تلفازية، إلا أن مثل هذا الإرهاب لن يكون له تأثير كبير.

عند احتجاز الرهائن من قبل الخاطفين يقوموا بنشر صوراً فوتوغرافية أو شرائط فيديو لضحاياهم بغض النظر عن جنسياتهم، ومثل هذه الصور والأشرطة غالباً ما يتلقفها الصحفيون بشوق شديد، لينشرونها على الصفحات الأولى من جرائدهم، كما يتم عرض شرائط الفيديو في نشرات التلفاز الإخبارية.

إذن تكنولوجيا المعلومات، وتحديداً تكنولوجيا الإعلام والاتصال تثير الرأي العام من خلال الصور وأفلام الفيديو، إذ تبدأ الصيحات المدوية لأقارب الضحايا تقلق مضاجع الحكومات، لكي تفعل أي شيء في سبيل الإفراج عن الرهائن(٢٠). أو وضع الحلول التي تحول دون قيام مثل هؤلاء المجرمين من ترويع الناس.

إن جريمة الإرهاب المعلوماتي أو الإلكتروني تتجسد في ثلاثة أنواع هي:

١- إرهاب ضد الأفراد:

المقصود به هو كل فعل يقوم به الفرد في تعامله خلال الإنترنت بشكل خاص وتكنولوجيا المعلومات بشكل عام، مهما كان صغيراً ، مسجل عليه، والكمبيوتر ذو ذاكرة حديدية لا تخبو ولا يعتريها النسيان، وكما هو واضح يمثل هنا تهديداً حقيقياً لهتك الخصوصية الفردية، بعد أن أصبح الممكن النفاذ إلى ما يتداوله البشر من أحاديث عبر هذه الشبكة، من حوار المناهضين لنظام الحكم إلى همس المحبيّن، وقد شهدت ساحة الإنترنت حالات عدة لـ (الإبتزاز المعلوماتي) من قبل أشخاص تمكنوا - بوسيلة أو بأخرى- من اصطياد رسائل البريد الإلكتروني أو التصنت على حلقات الدردشة عبر الإنترنت، وجدير بالذكر هنا أن أكثر برامج الدردشة شيوعاً، والمعروفة باسم (ICQ) هي من إنتاج شركة إسرائيلية، وقد تم اقتناؤها أخيراً من قبل كبرى شركات خدمات الإنترنت بأمريكا (أمريكا أون لاين Aol)، ومن السهولة بمكان النفاذ إلى كل ما تتضمنه حلقات الدردشة التي يشارك فيها المواطنون العرب لكشف ما يختلج بالصدور وما تبطنه السرائر.

ما يساعد على استخدام الإنترنت كوسيلة للابتزاز، التواصل عن بعد، إذ يتيح فرصاً عديدة لتقمص الشخصيات، وما أكثر ما تمقص الرجال شخصيات النساء، وتقمصت النساء شخصيات الرجال لخداع الآخرين والأخريات من أجل البوح بأسرار شخصية حسّاسة يمكن أن تستغل ضدهم أو ضدهن . علاوة على ذلك تتيح تكنولوجيا المعلومات وسائل مبتكرة للابتزاز نذكر منها على سبيل المثال: التهديد بالوثائق المزورة، والصور الفاضحة التي يتم تزييفها إلكترونياً بدرجة يصعب التفريق بينها وبين الصور الحقيقية. هذا بخلاف مصادر تهديد أخرى للنفاذ إلى الحسابات الشخصية، أو السرقة من خلال استخدام أرقام بطاقات الائتمان الخاصة بالغير في معاملات التجارة الإلكترونية.

ليس هناك حالياً من حل لحماية خصوصية الأفراد إلا باستخدام أساليب المحافظة على سرية البيانات (encryption)، إلا أن هناك لكل شفيرة سرية كما هو معروف وسيلة فنية لكسرها، فالأمر - على ما يبدو- في حاجة إلى صيغ جديدة يتآلف فيها الإلزام من خلال القوانين، مع الإلزام من خلال إشاعة قيم أخلاقية جديدة تتلائم ومطالب عصر المعلومات.

٢- **إرهاب المؤسسات:**

إن من أخطر مصادر التهديد الإلكتروني للمؤسسات هو اختراق شبكات اتصالاتها والنفاذ إلى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها المختلفة، وفي ظل المنافسة الشرسة التي تشهدها معظم الأسواق حالياً أصبح التجسس على أنشطة الشركات من قبل منافسيها عبر الإنترنت مصدر قلق حقيقي، وقد تم اختراق شبكات المعلومات لبعض البنوك السودانية في إطار الحملة التي شنت ضد السودان ضمن ما أسموه بتمويل العمليات الإرهابية.

لعل من المظاهر الأخرى لإرهاب المؤسسات معلوماتياً إسقاط موقع المؤسسة على الإنترنت، وذلك بأن يصوب إليه وابل من الرسائل المولدة تلقائياً التي تظل تنهمر إلى أن تصل إلى حد يعجز فيه الموقع تماماً عن ملاحقتها ليسقط وتسقط معه - بالتالي - جميع المعاملات التجارية والمالية التي يوفرها موقع المؤسسة لعملائه ووكلائه وشركائه.

أضف إلى ذلك، فإن من وسائل التهديد الأخرى التي تتعرض لها المؤسسات فك شيفرة حماية سرية البيانات التي تتبادلها مع الآخرين خارج المؤسسة من عملاء ووكلاء وما شابه، وقد سمعنا عن هذا الشاب النرويجي الذي أثار الرعب في قلوب أباطرة صناعة السينما في هوليود بعد أن نشر في الإنترنت برنامجاً من أسطر عدة يمكن به فك الشيفرة الرقمية التي تبث بها الأفلام عبر

الشبكة . إنه بحق ذكاء الأفراد في مواجهة سطوة المؤسسات، ولا جدال في أن هذه المعركة لا تزال في بدايتها، وستلقي بظلال كثيفة على ما يجري حالياً في مجال حماية الملكية الفكرية.

٣- إرهاب ضد الدول:

يتمثل الإرهاب الإلكتروني للدول في إمكان النفاذ إلى شبكات التحكم في المرافق العامة مما يتسبب في الشلل التام للبنى التحتية الأساسية، بل واحتمال تدميرها بالكامل، إن الدول باتت معرضة لما يمكن أن نطلق عليه أسلحة التدمير الشامل باستخدام الأسلحة البيولوجية المعلوماتية المتمثلة في جيوش الفيروسات التي تخترق حدود الدول لتشيع الخراب والفوضى في أرجاء البنية المعلوماتية، ومن قبيل المفارقة، فإنه كلما ارتقت الدول في استخدام شبكات نظام المعلومات وزاد الترابط بين هذه الشبكات، زاد تعرضها بالتالي لمثل هذا النوع من التهديد، وهو الوضع الذي يثير أشد القلق لدى الدول المتقدمة التي يتزايد اعتمادها على شبكات المعلومات في إدارة معظم شؤون حياتها. علاوة على ما سبق، هناك الإرهاب الإلكتروني غرضه الإضرار بالمصالح الاقتصادية للدولة. وقد مارست إسرائيل هذا النوع من الإرهاب بهدف تشويه صورة السياحة العربية.(٢١)

٢- جريمة تضليل العقول: تكنولوجيا الإعلام المزيف.

مما لا شك فيه أن تكنولوجيا المعلومات، وتحديداً تكنولوجيا الاتصالات، لعبت أكثر من دور فعاّل في المجتمع، وأثرّت في المجتمع بشكل مباشر سلباً وإيجاباً، وإذا كان الحديث عن الدور الإيجابي يدعونا إلى غض النظر عنه أحياناً، إلا أن الحديث عن الجانب السلبي لا يمكن تجاهله أو إغفاله أو غض الطرف عنه.

بقدر ما لعبت تكنولوجيا الاتصالات دوراً إيجابياً في المجتمع الإنساني، إلا أنها فعلت كذلك سلباً في المجتمع، عن عملية قلب العقول من خلال قلب وتزييف الحقائق عبر الطرق المستمر على أشياء غير موجودة، ومن ثم إظهار وجودها بشكل أو آخر أو من خلال الوعود الجديدة ومن ثم عدم تحقيقها، وجعل المواطن يعيش حالة من التأمل والترغيب لتنفيذ هذا الوعد أو ذاك، ويبقى المواطن يعيش في دوامة الوعود الكاذبة، وتضييع عليه حقائق الأمور؛ وكل ذلك يأتي من أجل تحقيق مكاسب لشخص أو فئة أو طبقة صغيرة على حساب المواطن العام.

وهذا التضليل جريمة بحد ذاتها، يجب أن يحاسب عليها القانون أو الأعراف والتقاليد إذا كنا نعيش في دول لا زالت تعمل فيها الأعراف والتقاليد أكثر من القوانين وما أكثر هذه الدول في عالمنا الجامد؟ وينطبق على هذه المجتمعات قول الشاعر :

فقهاء يا وطني نموت ... وقطارنا أبداً يفوت

عندما يعمد مديرو أجهزة الإعلام إلى طرح أفكار وتوجهات لا تتطابق مع حقائق الوجود الاجتماعي، فإنهم يتحولون إلى سائسي عقول. ذلك أن الأفكار التي تنحو عن عمد إلى استحداث زائف، وإلى إنتاج وعي لا يستطيع أن يستوعب بإرادته الشروط الفعلية للحياة القائمة أو أن يرفضها، سواء على المستوى الشخصي أو الاجتماعي، ليست في الواقع سوى أفكار مموزجة أو مضللة.

إن تضليل عقول البشر هو على حد قول (باولو فرير) : " أداة للقهر" . فهو يمثل إحدى الأدوات التي تسعى النخبة من خلالها إلى تطويع الجماهير لأهدافها الخاصة. فباستخدام الأساطير، التي تفسر وتبرر الشروط السائدة للوجود، بل تضفي عليها أحياناً طابعاً خلاباً، يضمن المضللون التأييد الشعبي لنظام اجتماعي لا يخدم في المدى البعيد المصالح الحقيقية للأغلبية. وعندما يؤدي التضليل الإعلامي للجماهير دوره بنجاح، تنتفي الحاجة إلى اتخاذ تدابير اجتماعية بديلة.

لا يمثل أحياناً تضليل الجماهير أول أداة تتبناها النخب الحاكمة من أجل الحفاظ على السيطرة الاجتماعية، فالحكام لا يلجأون إلى التضليل الإعلامي كما يوضح فرير إلا عندما يبدأ الشعب في الظهور (ولو بصورة فجة) كإرادة اجتماعية في مسار العملية التاريخية، أما قبل ذلك فلا وجود للتضليل بالمعنى الدقيق للكلمة، بل يجد بالأحرى قمعاً شاملاً، إذ لا ضرورة هناك لتضليل المضطهدين، عندما يكونوا غارقين لآذانهم في بؤس الواقع.

إن القمع في الواقع، أي كبت الفرد وإخضاعه كلية، لم يقتصر على أي كيان جغرافي أو سياسي منفرد، فأغلب البشر تعرضوا للقمع، على مر العصور وفي كل أرجاء العالم، من خلال وضع من الإفقار الكامل يطرح نفسه على أنه طبيعة، (ويكون ذلك صحيحاً في حالات قليلة) ، على أنه لا يعدو، في أغلب الحالات أن يكون النتيجة المترتبة على التقسيم الاجتماعي غير المتكافئ، فحتى وقت قريب لم يكن هناك سوى قلة نادرة من البلدان التي شاء لها حظها السعيد أن تجمع بين الموقع الجغرافي وكفاية المصادر الأولية والأسبقية التاريخية المواتية، مما وفر لها وسيلة الإفلات من مخاطر الندرة والكوارث الاقتصادية المتكررة، ومع ذلك فقد ظل القمع، حتى في تلك المواقع المتميزة نسبياً، قدر أغلب الناس حتى أواخر القرن الثامن عشر وأوئل القرن التاسع عشر.

إن التقسيم الثابت للمجتمع إلى فئتين عريضتين من (الرابحين) و(الخاسرين)، إنما ينشأ وتتوافر له عوامل الاستمرار نتيجة للحفاظ على نظام التملك الخاص للملكيات المنتجة والاعتراف به، بل وتقديس هذا النظام، وامتداد مبدأ التملك الخاص لجميع أوجه الوجود الإنساني الأخرى،

ويؤدي القبول العام بتطبيق هذا التنظيم على النشاط الاجتماعي لا محالة، على أن يحقق بعضهم نجاحا اقتصادياً، ثم إلى تعزيزهم لنجاحهم، وأخيراً إلى انضمامهم إلى المتحكمين في تشكيل وصياغة الحياة الاجتماعية. ويظل الآخرون أي الأغلبية، يمارسون أعمالهم بوصفهم ممتثلين لا أكثر، وبوصفهم محرومين ومضللين.. وهم يتعرضون (أو يتم إخضاعهم) للتضليل الإعلامي على وجه التحديد، من أجل الاستمرار في المشاركة (إن لم يكن بإخلاص تام فعلى الأقل بصورة إيجابية).

في روتين الحياة اليومية المقرر. ويقدم النظام لهم مقابلاً يكفي لاكتساب بعض مزايا الوضع الاقتصادي المقبول، في الوقت الذي يؤدي بهم التضليل الإعلامي إلى أن يراودهم الأمل في إمكان تحويل هذا الروتين الحياتي اليومي، إلى امتياز شخصي أكبر لأنفسهم ولأطفالهم.

عندما يكون التضليل الإعلامي هو الأداة الأساسية للهيمنة الاجتماعية، كما هو الحال في الولايات المتحدة ، تكون الأولوية لتنسيق وتنقيح الوسائل التقنية للتضليل على الأنشطة الثقافية الأخرى. من هنا تجتذب أنشطة التضليل الإعلامي، طبقاً للمبادئ السوق، أذكى المواهب؛ نظراً لأنها تقدم أعلى حوافز النظام . وهكذا ينتهي الأمر بالدارسين الموجودين من حاملي الدكتوراه في الأدب الإنجليزي إلى وظيفة محرر إعلانات، فشارع ماديسون يدفع أضعاف ما تدفعه أقسام اللغة الإنجليزية بالجامعة.

إن وسائل التضليل عديدة ومتنوعة ، لكن من الواضح أن السيطرة على أجهزة المعلومات، والصور على كل المستويات، تمثل وسيلة أساسية. ويتم تأمين ذلك من خلال إعمال قاعدة بسيطة من قواعد اقتصاد السوق. فامتلاك وسائل الإعلام والسيطرة عليها، شأن أشكال الملكية الأخرى، متاح لمن يملكون رأس المال. والنتيجة الحتمية لذلك هي أن تصبح محطات الإذاعة وشبكات التلفزه والصحف والمجلات، وصناعة السينما ودور النشر مملوكة جميعاً لمجموعة من المؤسسات المشتركة والتكتلات الإعلامية، وهكذا يصبح الجهاز الإعلامي جاهزاً تماماً للاضطلاع بدور فعال وحاسم في عملية التضليل (٢٢).

لأجل تحقيق جريمة التضليل الإعلامي في المجتمع التي تمارس عليه هذه العملية، تعمل وسائل الإعلام والقابعين خلف تكنولوجياتها على توجيه العقول نحو الخارج أحياناً، أي خلق أو تخليق ما يسمى بنظرية المؤامرة وبالتالي يُشغل المجتمع بكل فئاته، وتكرس جهوده لمواجهة هذا الخطر الوهمي القادم من الخارج، وبالتالي تذهب جهود الناس وطاقاتهم، وتصرف أموال طائلة ، الشعب أحق بها، على مشاريع وهمية كاذبة، وهذه تعد من أكبر الجرائم التي يجب أن يحاسب ويعاقب

عليها كل من مارس هذا الفعل الإجرامي، وكذلك الذي كان وراء دفع الأموال لهذه الأفلام غير الشريفة التـي قامـت بغسل وتغيير وتوجيه وتضليل عقول أبناء الشعب لاسيما الطبقة الفقيرة غير المتعلمـة، وذات التعلـيم المحـدود كـذلك . وكان من الأجدر بهذه الأفلام أن تدافع عن الحقوق العامة بدلاً أن تضيّعها من أجل كسب المال عـلى حـساب الطبقـات الفقيرة، وما أكثرها في عالم اليوم.

لكي يؤدي التضليل الإعلامي دوره بفعالية أكبر، لابد من إخفاء شواهد وجوده، شأنه بذلك شأن الجرائم التي تحصل في المجتمع، يحاول المجرم إخفاء آثار الجريمة أي أن التضليل يكون ناجحاً عندما يشعر المـضلَّلون بـأن الأشـياء هـي عـلى ماهية عليه من الوجهة الطبيعية والحتمية، بإيجاز شديد نقول: إن التـضليل الإعلامـي يقتـضي واقعـاً زائفـاً هـو الإنكـار المستمر لوجوده أصلاً.

لذلك بات لزاماً على الشعب الذي يجري تضليله، أن يؤمن بحياد مؤسساته الاجتماعية والرئيسة لابد مـن أن يـؤمن بأن الحكومة والإلام والتعليم والعلم بعيدة جميعاً عن معترك المصالح الاجتماعية المتصارعة.

إن سيطرة النخبة تقتضي تجاهل، أو تحريف الواقع الاجتماعي.

تستخدم تكنولوجيا الاتصالات في ارتكاب جريمة التضليل من خلال استخدام الأساطير مـن أجـل هـدف محـدد هـو السيطرة على الشعب وعندما يتم إدخالها على نحو غير محسوس في الوعي الشعبي، وهو ما يحدث بالفعـل مـن خـلال أجهزة الثقافة والإعلام، فإن قوة تأثيرها تتضاعف من حيث إن الأفراد يظلون غير واعين بأنه قد تم تضليلهم، وفضلاً عـن ذلك فإن عملية السيطرة تصبح أكثر فاعلية من خلال الشكل الخاص، الذي يجـري نقـل الأسـطورة مـن خلالـه. ذلـك أن تقنية النقل يمكن أن تضيف بذاتها بعداً جديداً إلى العملية التضليلية. والواقع أن شكل الاتـصال أو الإعـلام، عـلى النحـو الذي تطور به في البلدان التي يسود فيها اقتصاد السوق، هو تجسيد فعلي للتحكم في الوعي. وهـو مـا يمكـن ملاحظتـه بسهولة تامة في تقنية نشر المعلومات المستخدمة على نطاق واسع في أمريكا على سبيل المثال، ويلاحظ (فرير) أن إحدى السمات المميزة للعمل الثقافي القمعي، والتي لا يدركها أبداً المختصون، المخلصون والسذج في وقت معـاً، والمـشاركون في النشاط الدائر، هي التأكيد على النظرة التي تحصر المشكلات في بؤر (Focalized view)، بدلاً مـن رؤيتهـا بوصـفها أبعـاداً لكل واحد. (٢٣)

علاوة على ما سبق ، فإن تكنولوجيا الاتصالات تستخدم في تنفيذ جريمة تضليل العقـول مـن خـلال فوريـة المتابعـة الإعلامية. ترتبط الفورية الإعلامية ارتباطاً وثيقاً بعملية التجزيء، بل وتشكل

في الواقع عنصراً ضرورياً من عناصر وجودها، ويساعد هذا الطابع الآني اللحظي على تزايد القوة التضليلية لأجهزة الإعلام. ذلك أن المادة الإعلامية سريعة الزوال، لا تخلف وراءها أي بنية باقية أو ثابتة، لذا فهي تعوض أيضاً عملية الفهم، ورغم ذلك تظل اللحظية أو الفورية أي (تسجيل الأحداث والتعليق عليها فور وقوعها) من أهم مبادئ العديد من الصحف. وينظر إلى تلك الأنظمة الاجتماعية التي لا تقدم الإعلام الفوري، على أنها متخلفة بصورة ميئوس منها ومفتقرة إلى الكفاءة أو على أنها - وتلك تهمة أكثر خطورة - فاشلة اجتماعياً. فتكنولوجيا الاتصال، باستخداماتها الحالية، تروج لتوجهات بلا تاريخ ، وبالتالي فهي توجهات مضادة للمعرفة.

إن من السهل أن تتخيل نوع التصميمات الإلكترونية التي تستخدم فورية المتابعة، بوصفها إضافة وإكمالاً لبناء سياقات ذات معنى. لكننا لا نستطيع أن نعتقد بالسهولة نفسها أن فورية المتابعة، بوصفها أداة تضليل، وقد يتم التخلي عنها في الوقت الذي تخدم فيه سائسي العقول من خلال إعاقتها الفعالة للفهم الشعبي.(٢٤)

أما في العالم العربي، يتمثل دور التضليل الذي مارسه الإعلام العربي، بل يتأكد قولاً وفعلاً، من خلال غياب استطلاعات الرأي المرتبطة بالجانب السياسي على الساحة العربية، إذ لم نقرأ أو نسمع أو نشاهد يوماً من الأيام، استطلاعاً للرأي حول مثلاً، حقوق الإنسان في العالم العربي، أو صلاحية الرئيس ، أو نسبة رضا الشعب عن الحاكم أو الحكومة، بيد أننا نقرأ ونشاهد عبر مختلف وسائل الإعلام العربي وتكنولوجياته، أخبار التمجيد والانتصارات والإنجازات التي حققها هذا الحاكم أو ذاك ، والشعارات التي سعى ويسعى إلى تحقيقها، ولكن في حقيقة هذا الأمر إنها بعيدة عن الواقع جملة وتفصيلاً، ناسياً هذا الإعلام أو متناسياً أن مواطن اليوم في العالم العربي، يختلف عنه في الأمس، فبقدر ما كان مواطن الأمس يعيش في عزلة ، إذا صح القول، عزلة مارسها الإعلام العربي ذاته، فإن المواطن العربي اليوم يعيش في عامل واسع عريض لا يعرف الحدود ولا السدود، وذلك بفعل تكنولوجيا المعلومات (٢٥).

إن جريمة تضليل العقول تتم أيضاً في العالم العربي عبر استخدام تكنولوجيا الاتصالات عندما يتم تجاهل أو التغاضي الذي يمارسه الإعلاميون العرب عن المسكوت عنه والمتمثل في:

١- الاعتقال العشوائي للمشتبه بهم سياسياً.

٢- اعتقال الأقارب عسفاً إلى حين اعتقال المشتبه بهم .

٣- محاكمات سريعة أمام محاكم خاصة.

٤- قتل أو خطف الشخصيات المعارضة المعروفة.

٥- تعذيب المحتجزين لانتزاع التعريف.

٦- تعذيب سجناء الرأي.

٧- القتل الجماعي أو تدمير التجمعات التي يشتبه أنها عناصر المعارضة (٣٦)

٣- التزييف والتزوير:

نظراً للتطور التقني الهائل في أجهزة الكمبيوتر والطابعات الملونة وأجهزة المسح الضوئي، دخل الكمبيوتر وبتوسع في مجال التزييف والتزوير، حيث يمكن من خلاله نقل توقيع شخص ما على شيك أو إيصال أمانة أو عقد أرض أو شقة، كما يمكن استخدام الكمبيوتر في عملية تزييف العملات الورقية (العربية والأجنبية)، والمشكلة أن العملات المزيفة تكاد تتطابق تماماً مع النقود السليمة، ولا يمكن التعرف عليها من خلال خبرة فنية ومهارة عالية.

لعل من بين الأشكال الجديدة الجريمة التكنولوجية، تزييف التوقيع على الشيكات والمستندات والعقود، فمن خلال جهاز المسح الضوئي وطابعة الكمبيوتر يمكن للمزور أن يصل للتوقيع نفسه، فقد يضع الفرد توقيع على مستند ما، ويقوم المزور بالحصول على هذا التوقيع ويدخله إلى الكمبيوتر من خلال جهاز المسح الضوئي، ثم يقوم بطباعة التوقيع بالحجم واللون نفسه على عقد أو شيك أو أي مستند آخر.

لقد بلغ تزييف العملات الورقية درجة عالية من الإتقان في ظل الثورة التكنولوجية التي نعيشها، حيث يمكن إدخال وجه ورقة النقد وظهرها عن طريق جهاز المسح الضوئي إلى الكمبيوتر، حيث يتم استخدام برامج معالجة الصورة في تصحيح ألوان العملة الورقية بحيث تطابق الأصل تماماً ، وبعد ذلك يتم تكرار ظهر الورقة ووجها حسب مقاس الورق الذي تطبعه الطابعة ليتم طباعة أكثر من ورقة نقد على نسخ (فرخ) الورق الواحد ومن خلال استخدام طابعات الليزر الملونة (Lasercior printers)، يتم الحصول على النقود المزيفة بدرجة عالية من الدقة والإتقان.

تواجه رجال الأمن مشكلة حقيقية وهي أن المجرمين الجدد، الذين يقومون بمثل هذه العمليات القذرة هم من ذوي الياقات البيضاء سواء كانوا رجال أعمال أو مهندسي كمبيوتر أو أمناء شرطة وهذا من واقع الجرائم التي يتم مطالعتها في الصحافة اليومية. والمشكلة أيضاً هي اتساع دائرة التزوير والتزييف، مع صعوبة حصر القائمين بها في ظل انتشار أجهزة الكمبيوتر وملحقاتها، والغريب حقاً أنه ربما في بعض الدول غير مسموح بدخول طابعات الليزر الملونة لدى القادمين من الخارج، حيث لا يتم الإفراج عن مثل هذه الطابعات في الموانىء والمطارات إلا بعد

الحصول على موافقة العديد من الجهات ، وذلك حتى يتم الحصول على اسم الشخص وعنوانه للرجوع إليه عند حدوث بعض قضايا التزييف (٢٧)

٤- جريمة العبث بالبرامج أو جرائم تعمد الأذى والتدمير:

مما لا شك فيه أن جرائم تكنولوجيا المعلومات لا تأخذ شكلاً أو نوعاً واحداً، وإنما تختلف وذلك لإختلاف نوايا وسلوك المجرم ذاته، وجريمة العبث بالبرامج أو ما يسمى بجرائم تعمد الأذى والتدمير (Crimesof Malice and Destruction) ما هي إلا عبارة عن استخدام فيروس محدد لتدمير برامج معدة مسبقاً في حاسبات أخرى.

يعد الفيروس بمثابة برنامج يتم تصميمه بهدف الدخول إلى أجهزة الحاسوب وإحداث الأضرار بها وتزداد خطورة الفيروسات في ظل وجود شبكة المعلومات الدولية (الإنترنت)، نظراً لأنها تجمع الكمبيوترات ببعضها البعض، وتقع جرائم الحاسوب في الاستخدام غير المرخص لهذه الأجهزة أو البرامج بدون ترخيص أو عرقلة مستخدم من التوصل إلى حاسوبه أو برامجه أو بياناته أو موارد الشبكة، أو الاستخدام أو التآمر لاستعمال موارد الحاسوب للحصول بطرق غير قانونية، كذلك تصميم برامج التحطيم أو تغيير البيانات والبرامج والذاكرة والأقراص الصلبة (فيروس الحاسوب)، وهو مصطلح دخل حديثاً مجال صناعة الحاسوب ليقوم ببعض الأساليب الغادرة والماكرة التي يمكن عن طريقها غزو الحاسوب، وببساطة شديدة الفيروس هو برنامج حاسوب مثل أي برنامج آخر ولكنه يهدف إلى إحداث أكبر ضرر بنظام الحاسوب وله القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتياً، ويقوم الفيروس بالانتشار بين برامج الحاسوب المختلفة وبين مواقع مختلفة في الذاكرة (٢٨).

صفات الفيروسات:

١- القدرة على الاختفاء : فالفيروس ما هو إلا برنامج له القدرة على إخفاء نفسه عن المستخدم والتمويه عليه، والفيروس يستخدم وسائل متعددة في الاختفاء، منها ارتباطه بالبرامج الشائعة الاستخدام . حيث أن كل مستخدم للحاسب الشخصي يهتم بتوفير البرامج التي تمكنه من الاستفادة بخصائص الحاسب، وبعض المستخدمين يقوم بنسخ هذه البرامج دون السؤال عن مصدرها، وعند تشغيلها بنقل الفيروس إلى القرص، ويقوم بأداء أعماله التدميرية، وهناك فيروسات تدخل إلى الحاسب كملفات مختفية بحيث لا يستطيع المستخدم ملاحظة وجودها عن طريق فهرس الملفات، وبعض الفيروسات تقوم بالاستقرار في أماكن معينة يصعب على المستخدم ملاحظتها مثل الذاكرة وتنتظر في هذا المكان حتى

تشير الساعة إلى تاريخ معين فتقوم بتشغيل نفسها وتنفيذ أعمالها التدميرية، كما أن بعض الفيروسات تقوم بإخفاء أي آثار دالة على وجودها، حيث تظل البرامج المحتوية على الفيروس تعمل بكفاءة دون أخطاء مدة طويلة وفي نفس الوقت يقوم الفيروس بالانتقال من برنامج إلى آخر بخفة.

٢- الانتشار : لفيروس الكمبيوتر قدرة كبيرة جداً على الانتشار تفوق قدرة الفيروس البيولوجي، فيمكن لفيروس الكمبيوتر أن ينتقل إلى ملايين المستخدمين في نفس الوقت ويمكن في ثوان معدودة أن ينتقل من قارة إلى أخرى.

٣- القدرة على الاختراق: لفيروس الكمبيوتر قدرة على اختراق نظام المعلومات، وكذلك الموانع التي يقيمها المستخدم وغالباً ما يدخل الفيروس عن طريق حصان طروادة أو فيروس القدرة.

٤- القدرة على التدمير : عندما يدخل الفيروس إلى جهاز الكمبيوتر يظل ساكناً حتى تبدأ لحظة الصفر التي يبدي عندها في النشاط والحرة . وساعة الصفر هذه أما أن تكون كلمة معينة يمر بها مستخدم الكمبيوتر أو إشارة معينة أو عند تاريخ معينة من السنة ويعمل الفيروس على مسح البيانات المخزنة على الذاكرة (٢٩).

٥- خاصية التسلسل والعمل في الخفاء (stealth).

٦- خاصية التكاثر (Riplication)، ويعني بأن يصيب الفيروس جهاز الكمبيوتر ويقوم بنسخ نفسه مرات عدة بهدف الانتشار والالتصاق في الملفات المتناثرة على الاسطوانة (٣٠)

أشهر أنواع الفيروسات:

أما أشهر أنواع الفيروسات التي تستخدم في تنفيذ جريمة العبث بالبرامج أو جرائم تعمد الأذى والتدمير فهي:

١- **فيروس القردة: Nlonkeys:**

لم يعد هذا الفيروس خطير كما كان من قبل ، حيث يمكن للمستخدم بمجرد رؤية العلامات الدالة عليه أن يقوم بمسحه. وهذا الفيروس يقوم بعرض شاشة بها مجموعة من القرود التي تقوم بأعمال بهلوانية وأثناء قفز القرود على الشاشة فإن البرنامج يعمل نسخ من نفسه في أماكن متعددة كما يقوم بتدمير الفهرس الرئيس للقرص الصلب.

٢- **فيروس مايكل أنجلو Michael Anglo:**

يسمى هذا الفيروس بذلك الأسم لأنه لا يعمل إلا في يوم ٣/٦، وهو يطابق يوم عيد ميلاد الفنان مايكل أنجلو.

٣- **فيروس إسرائيل:**

وهو فيروس تم اكتشافه بالجامعة العبرية بالقدس عام (١٩٨٨)، ووصفته الصحف بالبرنامج القاتل أو مميت الكمبيوتر الأول، ويقوم هذا الفيروس بإبطاء تشغيل النظام إلى نصف زمن التشغيل تقريباً بعد نصف ساعة فقط من تشغيل الجهاز.

٤- **فيروس كاوت عيد الميلاد: Christian card:**

ظهر هذا الفيروس في إيران، وهو ينتشر عن طريق ارساله بالبريد الإلكتروني وهو يعرض كارت عيد الميلاد على الشاشة، وفي نفس الوقت يقرأ الملفات التي تحتوي على عناوين المشتركين في الشبكة ويرسل نسخ من نفسه إلى هؤلاء المشتركين.

٥- **فيروس الجنس:**

يقوم هذا الفيروس ببعض الأعمال الجنسية المثيرة والتي تثير مشغل جهاز الكمبيوتر وأثناء انشغال مشغل الجهاز بمشاهدة هذه الأفعال الجنسية يقوم الفيروس بنسخ نفسه داخل القرص، وبعد فترة وجيزة يكون قد مسح جدول توزيع الملفات (٣١)

يضاف إلى تلك الأنواع ، أنواع أخرى من الفيروسات ، وربما ظهرت لاحقاً وستظهر مستقبلاً أنواع أخرى ربما يصعب الاستدلال عليها الهدف منها ارتكاب المزيد من جرائم التدمير والعبث ببرامج الكمبيوتر، ولذلك بات على مستخدمي الحاسبات الإلكترونية التعرف عليها من خلال زيادة المعرفة الثقافية في مجال جرائم تكنولوجيا المعلومات.

كيف ترتكب جرائم العبث بالبرامج؟

يؤدي الفيروس دائماً إلى تعديل البرامج، ومن ثم يقوم بالانتقال من برنامج بعد إصابته إلى برنامج آخر وتكون البرامج هي الوسيط الذي ينتقل من خلاله الفيروس، وعادة ما يقوم الفيروس بنسخ أوامر بدلاً عن أوامر البرنامج وبذلك يصبح البرنامج الأصلي غير قادر على تنفيذ أوامره الأصلية ويسبب الفيروس أضراراً بالغة بالبرامج ومنها تدمير قطاع التحميل وسرقة وقت الحاسوب، ويؤدي وجود الفيروس في بعض الأحيان إلى تقليل سرعة الحاسب ومن ثم يستغرق البرنامج وقتاً أطول في التنفيذ، وقد يكون ذلك غير ملحوظ في حالة البرامج التي يتم تنفيذها في وقت قصير،

ولكن تظهر في حالات أخرى مثل البحث في سجلات قاعدة بيانات وتصبح ملحوظة ومـؤثرة ويترتـب عليهـا تكلفـة مادية.

بدأت على سبيل المثال ألوف أجهزة الحاسوب المتـصلة بالـشبكة في الثـاني مـن نـوفمبر عـام (١٩٨٨)، بـدأت تتباطـأ حركتها وانتهى الأمر بالعديد منها إلى التوقف التام وعلى الرغم من أنه لم تدمر أية بيانات فقد ضاعت ملايين الـدولارات من زمن العمليات الكمبيوترية . ولقد أتضح في النهاية أن السبب فيما حدث هـو برنـامج كمبيـوتر مـؤذ أطلقـت عليـه تسمية (الدودة)، والذي انتشر من كمبيوتر إلى آخر عبر الشبكة وقد وصف على أنه دودة، وليست فيروسا، لأنه لم يكـن يصيب البرامج الأخرى، واتضح أن (روبرت موريس) ذا الثلاثة والعشرين ربيعاً والمتخرج في جامعة (كورنيل) هـو مـصمم الدودة، وقد أدين موريس بتهمة انتهـاك القـانون الـصادر عـام (١٩٨٦) والمتعلـق بالاحتيـال وسـوء الاسـتخدام في مجـال الكمبيوتر والذي يعد جريمة فيدرالية وعوقب بالسجن لمـدة ثـلاث سـنوات مـع وقـف التنفيـذ وإيقافـه تحـت المراقبـة وغرامة عشر آلاف دولار وأربعمائة ساعة عمل في الخدمة المجتمعية (٣٢). وقد يكون الإتلاف أما عن عمد وقـصد، وأمـا أن يكون بغير قصد.

كما أن الإتلاف قد يكون كلياً ويتمثل ذلك في محو البرامج والمعلومات المخزنـة داخـل الجهـاز كليـاً، وأمـا أن يكـون الإتلاف جزئياً ويطلق عليه تشويه أو تعييب ، ويتمثل ذلك في إدخال فيروس داخل الجهاز بحيث يعمل على التقليل من كفاءته أو بطء حركة الجهاز.

طرق ارتكاب جريمة الإتلاف:

يمكن القول : إن جرائم تكنولوجيا المعلومات هي من أنواع الجرائم الناعمـة إذا جـاز التعبـير، ومـن يرتكبهـا عـادة يكون من الأشخاص الأذكياء، والذكاء هنا يتجسد ربما من خلال وقت ارتكاب الجريمة إذ عادة ما ترتكب الجـرائم جريمـة تكنولوجيا المعلومات، يمكن أن يقوم بها وسط النهار وبين العشرات من الناس الجالسين في صالات ومقاهي الإنترنت.

أما بالنسبة للكيفية التي يتم عن طريقها إتلاف البرامج والمعلومات من عـلى الجهـاز، هنـاك العديـد مـن الوسـائل والطرق منها:

١- استخدام برنامج القنبلة المنطقية:

القنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة المعلومات بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع. ومن ذلـك مـثلاً إدخال تعليمات في برنامج نظام التشغيل وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرنامج المراد تنفيـذه. وهـو الذي ينفذ في كل مرة

عمل جديد وينصب البحث على عمل معين يمكن أن يكون محل الاعتداء . كأن تسعى القنبلة المنطقية إلى البحث عن حرف معين وليكن حرف (الألف) في أي سجل يتضمن أمر بالدفع وعندما تكشفه تتحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل. ومن الأمثلة الواقعية التي استخدمت فيها القنبلة المنطقية الآتي:

أ- تمكن خبير في نظام المعلومات في الدنمارك من وضع قنبلة منطقية في نظام إحدى الحاسبات أدت إلى محو أكثر من مائة برنامج، وقد تم أيضاً محو النسخ الاحتياطية عند تشغيلها نظراً لانتقال آثار القنبلة إليها، وتم ضبط المجرم وحكم عليه القضاء الدنماركي بالحبس لمدة سبعة أشهر.

ب- تمكّن كذلك أحد العاملين في ولاية لوس أنجلوس بالولايات المتحدة الأمريكية بإدارة المياه والطاقة من وضع قنبلة منطقية في نظام الكمبيوتر الخاص بها مما أدى إلى تخريب هذا النظام مرات عدة.

٢- استخدام برنامج القنبلة الزمنية:

هي عكس القنبلة المنطقية فهي تنطلق أو تنفجر في زمن وتاريخ محدد من السنة فهي مرتبطة بالزمن، فيمكن إدخالها في برنامج وضبطها لكي تنفجر مثلاً في يوم ٢٠٠٦/٥/١٥ الساعة (٣.١٥) ، وذلك بغرض تحويل نقود من حساب شخص معين لآخر. ومن الأمثلة الواقعية التي استخدم فيها أسلوب القنبلة الزمنية:

أ- قام خبير في فرنسا في نظم المعلومات بدافع الانتقام على أثر فصله من المنشأة التي يعمل بها بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة بحيث تنفجر بعد مضي ستة أشهر من رحيله عن المنشأة وترتب على ذلك إتلاف كل البيانات المتعلقة بها.

ب- قام في ألمانيا مبرمج بزرع البرنامج الذي يعمل القنبلة الزمنية في نظام المعلومات الخاص بالشركة التي يعمل بها وتم برمجة القنبلة بحيث يتعين أن تنفجر بعد عامين من فصله من الشركة، وفي حوالي الساعة الثالثة مساء حدث في اليوم الموعود أن أنهار نظام معلومات الشركة وظلت أكثر من (٣٠٠) طرفيه معطلة لبضعة أيام.

٣- استخدام برنامج الدودة

هي عبارة عن برنامج يستغل أي فجوات في نظام التشغيل كي ينتقل من حاسب آلي إلى آخر أو من شبكة إلى أخرى عبر المواصلات التي تربط بينهما. وتتكاثر أثناء عملية انتقالها كالبكتيريا

بإنتاج نسخ منها، ويهدف هذا البرنامج إلى شغل أكبر حيّز ممكن من سعة الشبكة ومن ثـم العمـل عـلى تقليـل أو خفض كفاءتها وأحياناً تتعدى هذا الهـدف لتبـدأ بعـد التكـاثر والانتـشار في التخريـب الفعـلي الملفـات والـبرامج ونظـم التشغيل.

من أمثلة برنامج الدودة ما يعرف بـ (Inter warm) والتي عن طريقها تمكن طالب أمريكي يدعى "روبرت مـوريس"، وهو طالب دراسات عليا في "جامعة كورنيل" بولاية نيويورك مـن تـدمير (١٦٠٠) شـبكة حاسـب آلي منتـشرة في الولايـات المتحدة. وترتب على هذا الهجوم خسائر تمثلت في تأخير الأبحاث آلاف الساعات وفي إعادة البرمجة بتكاليف بلغت عدة ملايين من الدولارات.

تم كذلك اكتشاف حالة جديدة من برامج الدودة وأطلق عليها مصطلح الـبرامج الدوديـة ضـد القتلـة، مـستخدمي الذرة ويرمز لها بـ (Wank) حيث غزت مرتين خلال عام (١٩٨٩) شبكة علوم الأرض والفضاء بالولايات المتحدة الأمريكيـة كنوع من الاحتجاج على اطلاق مكوك فضائي يعمل مجساً فضائياً مغطى ببودرة نووية.(٣٣)

وسائل انتقال العدوى بالفيروس:

مما لا شك فيه أن تكنولوجيا المعلومات باتت مسيطرة على أغلب نواحي الحياة، وذلك ربما يعد أمراً طبيعيـاً؛ لأنهـا أينما حلت وارتحلت عملت على إحلال قفزة نوعية في تلك الأعمال، مما فرض على الناس التمسك بها، بل والبحث عنهـا عندما تكون بعيدة عن متناول ذلك، بيد أن الأمر لا يخلو من السلبيات، وهكذا هي سنة الحياة، يُعد فيهـا الكـمال لله – سبحانه وتعالى– أدى التطور الحاصل في تكنولوجيا المعلومات إلى سرعة انتقال الأضرار من مكان بعيد إلى أمـاكن أخـرى، ربما أكثر بعداً، ويصعب على المجرم الوصول إليها بالطرق العادية، حيـث تأخـذ وقتـاً كبـيراً وجهـداً أكـبر وتكلـف مبـالغ طائلة، لكن عندما يكون فعل ارتكاب الجريمة عبر تكنولوجيا المعلومات، ارتكاب جرائم في أماكن بعيدة وهم جالسين في بيوتهم. ومن أهم الوسائل والأدوات التي تساعدهم على انتقال فعلهم الإجرامي هي:

١- البريد الإلكتروني:

يمكن ادخال الفيروسات عن طريق البريد الإلكتروني (E-mail) ويستخدم في ذلك فيروس كارت عيد الميلاد.

٢- الإرهاب:

تقوم الجماعات الإرهابية المنتظمة باستخدام نظم الاتصالات الحديثة في تنفيذ مخططاتها الإرهابية عـن بُعـد، كـأن تقوم بتفجير طائرة أو مطار أو منشأة عسكرية أو غير ذلك من الأماكن الاستراتيجية مـن عـلى بُعـد. ويـستخدم في ذلـك الفيروس الإسرائيلي.

٣-   نسخ البرامج:

يتم انتقال الفيروس إلى البرنامج أو المعلومات داخل الكمبيوتر عن طريق إدخال برنامج منسوخ إلى الجهاز فينتقل العدوى إلى البرامج والمعلومات.

٤-   تحميل برامج من الشبكات:

قد يؤدي تحميل برامج من الشبكات إلى الإصابة بالفيروس و إتلاف البرامج والمعلومات المخزنة داخل الكمبيوتر، ومن هذه البرامج، برامج ضغط البيانات (Comperssion)، حيث كثيراً ما يستخدم المشتركون هذه البرامج في ضغط البيانات لتوفير مساحات تخزينية وفي نفس الوقت نقل البيانات وغالباً ما تكون هذه البرامج محملة بالفيروس. لذلك يجب على المشترك أن يتأكد أن جميع المشتغلين داخل الشبكة معتمدين.

٥-   التخريب بواسطة الموظفين:

غالباً ما يتم تخريب وإتلاف البرامج والمعلومات بواسطة العاملين على جهاز الكمبيوتر؛ وذلك إما أن يكون بباعث الانتقام أو إثبات المهارة والكفاءة.

٦-   الجاسوسية :

غالباً ما تحاول أجهزة المخابرات أو الشركات الصناعية إلى إدخال فيروس إلى البرنامج المراد التجسس عليه؛ وذلك للحصول على معلومات عسكرية أو صناعية.(٣٤)

٥- جرائم السرقة الإلكترونية:

يمكن أنْ نصف جريمة السرقة بأنها عبارة عن قيام السارق (المجرم) بعمل أو أعمال ينتج عنها الاستيلاء أو السيطرة على حقوق الآخرين، أما جرائم السرقة التي تتم عن طريق تكنولوجيا المعلومات، هي تلك الجرائم التي يتم عبرها السيطرة أو الاستيلاء على معلومات فكرية مملوكة للغير، أو الاستيلاء على دسكات أو أقراص مكتنزة تتضمن معلومات وبيانات أنتجها الآخرون وكل هذه الأفعال الإجرامية تكون بواسطة تكنولوجيا المعلومات.

أما أنواع جرائم السرقة عبر تكنولوجيا المعلومات يمكن أن نذكرها بالشكل الآتي:

١-   سرقة الأقراص الصلبة:

إن سرقة الأقراص الصلبة يمكن أن تتراوح بين سرقة إحدى ملحقات الكمبيوتر في محل لبيع أجهزة الكمبيوتر ونزع تليفون خلوي (Culler phone) من سيارة شخص ما، وقد يقوم المجرمون

المحترفون بسرقة شحنات من رقائق الكمبيوتر الدقيقة، التي تقوم بعديد من المعالجات (Microprocsser chips) من على أرصفة شحن السفن وتفريغها في الموانئ أو من المراكز التجارية الضخمة.

إحدى الحالات المثيرة - بصفة خاصة في هذا السبيل - كانت سرقة كمبيوتر من سيارة ضابط بريطاني، وقد تصادف أن هذا الكمبيوتر كان يحتوي على خطط الجنرال الأمريكي نورمان شورزكوف (Norman schwarzkoph) التمهدية لغزو العراق، وتبين فيما بعد أن هذه الخطط لم تكن متوافقة مع ما تم بالفعل في أثناء الحرب. وقد أصبحت سرقة أجهزة الكمبيوتر مشكلة كبيرة في عديد من حرم الجامعات، وغالباً ما يقوم اللصوص الذين قد يكونوا محترفين بسرقة وحدة النظام (System unit)، ولا يأخذوا الأجزاء الخارجية من أجهزة الكمبيوتر.

٢- سرقة الأقراص المرنة:

يمكن أن تأخذ سرعة الأقراص المرنة شكلاً مادياً، مثل أن ينسل شخص هاربٌ بالأقراص المرنة لشخص ما، ولكن الأكثر احتمالية هو القيام بنسخ برامج الكمبيوتر. ومن هنا، يبحث منتجو البرامج عن الشركات التي تشتري نسخة واحدة من البرنامج، وتنسخ منها نسخاً بعدد أجهزة الكمبيوتر التي تملكها، ويقوم بعض المتعاونين الذين يتقاضون أجراً والدارسين بالإفشاء عن عديد من قراصنة البرامج "للبوليس المختص بمكافحة هذه القرصنة"، "Sefteare publishers"، وذلك للحث على مكافحة القرصنة في هذا المجال. وفي منتصف (١٩٩٤)، أتهم طالبان جامعيان بريطانيان بدعوى استخدام شبكة الانترنت؛ لتشجيع تبادل برامج الكمبيوتر، التي تمتع بحماية حق المؤلف.(Copyrighted software).

من الأنماط الأخرى لسرقة البرامج القيام بنسخ أو تزوير البرامج الشهيرة؛ مثل: "دوس" و "وندوز" "Windowa"، وغيرها وغالباً ما يقوم هؤلاء القراصنة بعملهم في تايوان والمكسيك وروسيا ومناطق عديدة من آسيا وأمريكا اللاتينية (وكذلك أمريكا الشمالية ودول أوروبا". وفي بعض البلدان، فإن أكثر من (٩٠%) من برامج الكمبيوتر الأمريكية المستخدمة بالفعل يُعتقد أنه قد تم نسخها بشكل غير قانوني.

٣- سرقة الوقت والخدمات:

هناك تصور كبير لدى العديد من الناس أن سرقة الوقت والخدمات من خلال تكنولوجيا المعلومات، لا تعد جريمة وفق مفهوم الجرائم، بيد أن الأمر يبدو معكوساً تماماً لهذا المفهوم، فمن المحتمل أن سرقة وقت الكمبيوتر تعد من الجرائم الأكثر شيوعاً مما قد يعتقده بعضهم،

وأكبر استخدام لهذا النوع من السرقات يتم من قبل أناس، يستخدمون الكمبيوتر في أماكن العمل لممارسة الألعاب المختلفة على أجهزة الكمبيوتر، كما قد يقوم البعض أيضاً بأعمال إضافية خاصة إلى جانب العمل الأصلي.

زادت سرقة الخدمات الكابلية والتلفازية عبر السنوات الماضية وقد أوردت شركة مونتجمري للتلفاز الكابلي الأمريكية (Cabletv Montgomery) تقريراً يفيد بأنها تخسر (١٢) مليون دولا سنوياً يكسبها القراصنة التي تبثها الشركة. ووفقاً للقانون الفيدرالي الأمريكي .. فإن المشاهد الذي يمتلك جهازاً غير شرعي لفك الشيفرة (Illegal decoder box)، يمكن أن يعرض نفسه للحبس ستة أشهر، ودفع غرامة قدرها ألف دولار.

عانت شركات التيلفون من سرقة الخطوط التليفونية ولسنوات عديدة وحديثاً جداً، اكتشفت هذه الشركات أن اللصوص قد وجدوا وسائل للدخول في نظم البريد الصوتي (voic – mail system) لها، وحينئذ يمكنهم إجراء المكالمات الخاصة بالمسافات الطويلة على حساب الشركة، كما وجدوا ايضاً وسائل التسلل إلى شبكات التليفون الخلوي لإجراء مكالمات مجانية، وفي عام (١٩٩٢) نجحت مجموعة من الشباب في الوصول إلى شبكة كمبيوتر واسعة الاستخدام، تُدعى (دتايمت) Tyment والشبكة الخاصة ببنك أوف أمريكا Bank of America ومن خلال هاتين الشبكتين، استطاع هؤلاء الشباب التسلل إلى المزيد من شبكات الكمبيوتر (٣٥).

٦- جريمة سرقة البيانات والأصول:

عادة تشمل سرقة الحاسب والتي تسمى قانونياً إختلاساً، أحد العاملين الموثوق بهم الذي لا يستطيع مقاومة إغراء السرقة، وفي أغلب الأحيان، يمكن القيام بالسرقة بسهولة مدهشة، مثال ذلك، استخدام رئيس مجلس الإدارة ومنفذو الإدارة العليا للشركة الأمريكية المعروفة باسم (Equity Funding corporation)، وهي شركة عامة للتأمين والتمويل المزدوج، النهايات الطرفية في إدخال بوالص تأمين لأناس وهميين، وبإدخال بيانات وهمية على مدار فترة تقدر بالسنوات، زادوا من أصول الشركة الظاهرة بشدة. ومن (٩٧.٠٠٠) بوليصة تأمين يحفظها الحاسب، كان حوالي ثلثيها بوالص خيالية تبلغ قيمتها (٢.١) بليون دولار! ونظراً لظهور الشركة بأنها تحقق ربحاً أكثر من الريح الحقيقي، فقد كانت أسهم الشركة مبالغ فيها بصورة كبيرة، وبالتالي، كان المتآمرون وهم من كبار أصحاب الأسهم قادرين على بيع حصصهم بأرباح معتبرة. وقد ظلت الخدعة مختفية لأن مراجعي الحسابات كانوا يقبلون مطبوعات الحاسب والتي كانت تسرد

أصحاب البوالص بصورة منسقة، ولم تكتشف الجريمة إلا بعد أن كشف أحد العاملين السابقين المخطط، وأصبحت هذه قضية كلاسيكية لمدى سهولة استخدام إمكانية التحايل بالحاسب إذا لم تطبق مراقبات مناسبة.

ومع تكاثر مستخدمي الانترنت، زادت مشكلات الفيروسات وسرقة الوثائق، ويعد تشفير المنقولات وتعليم الناس من الحاجة إلى حماية نظم البرامج من الفيروسات طرقاً مستخدمة لتخفيف المشكلة (٣٦).

٧- جريمة السطو على بطاقات الإئتمان والتجارة الإلكترونية:

عانت وتعاني العديد من المصارف في العالم مشكلة الاستخدام غير المشروع لبطاقات الإئتمان؛ نظراً لما يترتب على ذلك من خسائر مالية فادحة وتهديد لسمعة تلك المصارف ومساس بثقتها الإئتمانية (٣٧). ولذلك تعد عمليات السطو على بطاقات الإئتمان أحدث أنماط السلوك الإجرامي التي ارتبطت بشبكة الانترنت من بنوك أو مؤسسات مالية وأفراد، وقد زاد خطر انتشار هذا النوع من الجرائم لصعوبة التوصل إلى مرتكبيها، ففي كثير من الأحيان يكتشف حامل بطاقة الفيزا في دولة ما أن بطاقته قد استخدمت في شراء سلعة من أحد المحلات في دولة ثانية ويكون الفاعل في دولة ثالثة، وقد تمت الواقعة من خلال موقع المحل البائع على شبكة الانترنت(٣٨).

كيف تتم جريمة السطو؟

لعل الأثر الكبير الذي تلمسته الإنسانية وعاشته فوق أرض الواقع من خلال استخدام تكنولوجيا المعلومات، وهو ذلك الحدث الكبير الذي تمثل بوجود مصارف بلا صرافين، ووجود أموال ونقود تنتقل بومضة الكهرباء من بلد إلى آخر، وهذا الأمر الإيجابي الكبير الكبير تطور إلى حالة أكثر رقياً، تمثلت بوجود بطاقات الإئتمان . وهذه البطاقات منها أنواع عديدة كبطاقات السحب التي عن طريقها يسحب العميل مبالغ نقدية من حسابه، وقد تكون بطاقات ضمان شيكات؛ وذلك كضمان للشيكات التي يحررها حامل البطاقة خصماً من حسابه بالبنك صاحب البطاقة وهناك بطاقات إئتمان تعطي صاحبها تسهيل إئتماني من البنك مصدر للحامل الشرعي لهذه البطاقة، هذا هو الوجه المشرق للبطاقات المختلفة. ولكن رغم مزايا هذه البطاقات وانتشارها، فهي تمثل خطراً على التجارة الإلكترونية، ويتم التلاعب فيها عن طريق الانترنت، ويأخذ هذا التلاعب صوراً عديدة منها:

١- الحصول على بطاقة إئتمانية صحيحة بناءً على مستندات مزورة.

٢- قيام حاصل البطاقة باستعمالها بعد انتهاء مدة صلاحيتها أو بعد تنبيه البنك عليه بعدم استخدام البطاقة.

٣- التقاط الغير للبطاقة عند العثور عليها وهي مفقودة أو سرقتها وإساءة استعمالها.

٤- وقد يتلاعب موظف البنك ذاته ببيانات البطاقة بالاتفاق مع العميل حامل هذه البطاقة أو مع العصابات الإجرامية التي تتعامل في سرقة الأموال من البنوك عبر الانترنت وذلك عن طريق مدهم ببيانات بطاقات الوفاء أو السحب أو الائتمان الصحيحة لاستخدامها في تقليد أو اصطناع هذه البطاقات.

بيد أن جرائم التجارة الإلكترونية ليست قاصرة فقط على بطاقات الإئتمان وإن كانت الصورة الغالبة لهذه الجرائم، لا سيما وأنها تستهدف أموال هذه التجارة، لكن هناك صوراً أخرى تستهدف بيانات هذه التجارة ومواقعها على شبكة الانترنت، ولذلك فمن الجرائم الأخرى التي تتعرض لها بيانات التجارة الإلكترونية، هو الدخول غير المشروع إلى مواقع التجارة الإلكترونية على شبكة الإنترنت.

يتمثل السلوك الإجرامي في هذه الجريمة في الدخول - غير المشروع - على نظم معالجة البيانات، وكذلك إعاقة أو تحريف تشغيل نظم معالجة البيانات، وكذلك التلاعب في بيانات نظم معالجة هذه البيانات، وهذه الصور للسلوك الإجرامي تندرج ضمن جريمة يطلق عليها - جرائم الاعتداء على نظم المعالجة الآلية للبيانات - والتي تقع على مواقع التجارة الإلكترونية أو غيرها من المواقع على شبكة الإنترنت.

من صور الاعتداء غير المشروع على مواقع التجارة الإلكترونية، التعدي على البيانات الشخصية أو الاسمية التي تتعلق بهذه التجارة، ذلك أنه من الطبيعي أن يتم أثناء إجراء المعاملات الإلكترونية تبادل لبيانات تتعلق بالأشخاص، ومنهم العملاء الذين يطلبون سلعاً وخدمات، كما أن بعض هذه البيانات تتعلق بالمشروع والقائمين عليه والسلع والخدمات التي يسوقها، ولذلك فإن الأموال المتداولة في التجارة الإلكترونية قد تكون محلاً للسرقة أو الاحتيال أو خيانة الأمانة، وطالما أن هذه الأموال تتداول بطريق الإنترنت، ومن ثم فهي تتعرض للاعتداء من مخترقي الشبكات سواء كانوا من الشباب أو الأحداث.

أضف إلى ذلك، فإن جريمة السطو والسرقة تتم من خلال شبكة الانترنت بوصفها سوقاً مفتوحاً للبيع والشراء، حيث يتمكن التاجر من الإعلان عن سلعته بالصوت والصورة، ولديه الفرصة لإجراء مقارنة بين كل السلع المتاحة في كل أنحاء العالم، وللعميل أن يختار ما يريده

وتصله السلعة إلى منزله، ويقوم الحاسب الآلي بالتحري عن بطاقة الإئتمان البنكية وخصم قيمة من حساب المستهلك في أي بنك بالعالم أو أخطاره بأن حسابه لا يكفي. وهناك في ظل التجارة الإلكترونية، نظم للتحويل الإلكتروني للأموال، وأياً كانت درجة الأمان فمن الممكن اختراقها للحصول على أرقام بطاقات الإئتمان والتلاعب فيها أو لتحويل الأموال إلى المخترق ذاته بدلاً من أن تحول إلى الحساب الصحيح للعميل، وعملية الاستيلاء على أموال هذه التجارة عن طريق الشبكة من الجرائم الشائعة.

كذلك فإن الاستيلاء على أموال التجارة الإلكترونية بطريق الاحتيال - النصب - من الأموال التي أثارت جدلاً لدى الفقه والقضاء لكن غالب الرأي لديهما يرى أن الاحتيال للاستيلاء على أموال التجارة الإلكترونية أمر شائع الوقوع، وفي كل الدول، حيث يتم التدخل مباشرة في المعطيات أو البيانات، بإعطاء بيانات وهمية أو بتعديل البرامج أو عن طريق خلق برامج جديدة يكون الهدف منها الاستيلاء على الأموال بطريق الاحتيال، ولعل اساءة استعمال بطاقات الإئتمان من قبل الغير تعكس مدى سهولة الاستيلاء على أموال هذه التجارة بطريق النصب.

هناك عشرات الجرائم التي ارتكبت سواء في مجال السطو على بطاقات الإئتمان أو السطو على بيانات التجارة الإلكترونية، من خلال الدخول غير المشروع إلى مواقع التجارة الإلكترونية على شبكة الانترنت، فعلى سبيل المثال، اكتشف في عام (١٩٩٨) أحد البنوك الوطنية أن كمية كبيرة جداً من بطاقات عملائه تم استخدامها في التعامل على شبكة الانترنت وأن عملاء البنك قد اعترضوا على تلك العمليات ونفوا قيامهم بإجرائها، وقد اتضح بعد الفحص والتحري أن شابين أحدهما طالب والآخر كان يعمل بإحدى الشركات المتخصصة في تقديم خدمات الإنترنت في بور سعيد قد تمكنا من الحصول على أرقام بطاقات إئتمان عملاء البنك من خلال أحد مواقع القرصنة على شبكة الانترنت، وقام المتهمان باستخدام أرقام تلك البطاقات في التعامل بها عبر الشبكة، وقد بلغت جملة ما قاما بالاستيلاء عليه بالأسلوب المشار إليه حوالي نصف مليون دولار أمريكي.

نجد أن منافذ الصرف الإلكترونية ((automatic teller machines > (ATM وبطاقات الائتمان قد أصبحت مراكز جذب للأنشطة الإجرامية، وأن الحاجة لتأمين أقوى لتمثل محركاً آخر مهماً لتلك التكنولوجيا، حيث أصبحت بطاقات الشريط المغناطيسي ذات سمعة سيئة لكونها سهلة التقليد، وتختلف البطاقات الذكية عن البطاقات الممغنطة في أنه مستحيل قراءتها لغير المصرح له - أضف إلى تلك الجرائم، هناك جرائم أخرى لا تقل أهمية عن سابقتها، إذ

استطاع موظف يعمل على الحاسوب في متجر كبير بولاية أوكلاند، أن يغير في عناوين بعض العمـلاء ليوجـه بـضاعة قيمتها آلاف الدولارات على عناوين شركاء له في الجريمة، حيث إن شبكة الإنترنت قد فرضت على مجتمعاتنا أمـراً واقعـاً جديداً أفرز أنماطاً إجرامية وسلوكية لم تكن معروفة من قبل كان أهمها الاحتيال باستخدام أرقام بطاقـات الإئـتمان عـبر الشبكة، حيث اتضح أنها ظاهرة منتشرة على نطاق واسع بين شباب الجامعات ومدارس اللغات لا سـيما في ظـل شـعور سائد لدى هؤلاء الشباب باستحالة التوصل إلى مرتكبي تلك الأفعال (١١٠).

٨- جريمة الانتحال:

مما لا شك فيه أن جريمة الانتحال ليست من الجرائم الحديثة على المجتمعات الإنسانية، حيـث إنهـا موجـودة منـذ قديم الزمان، والدليل على ذلك وجود العديد من القوانين التي وضعت قديماً لمعالجـة هـذا النـوع مـن الجـرائم، إلا أن الجديد في جرائم الانتحال، إنها تجسدت بعمق جديد وأخذت بعداً جغرافياً جديداً، وذلك كله تحقـق بفعـل تكنولوجيـا المعلومات التي شكلت ظاهرة العصر الجديد.

يمكن تعريف جريمة الانتحال بأنها تجريد كاتب آخر من كتاباته أو تفسيراته أو النتائج التي كـان قـد توصـل إليهـا، وتقديمها على أنها ملك لشخص آخر.

بيد أن تكنولوجيا المعلومات تضع وجهاً جديداً للمنتحـل بأسـلوبين مختلفـين، فمـن جهـة تتـيح هـذه التكنولوجيـا للمنتحلين فرصاً جديدة ليمضوا في طريقهم للنسخ غير المصرح به، ومن جهة أخرى أخرى تتيح التكنولوجيـا ذاتهـا طرقـاً جديدة للإمساك بالأفراد الذين يسرقون المواد المتعلقة بأشخاص آخرين.

لعل واحدة من الأدوات والوسائل التي يتم استخدامها لارتكاب جرائم الانتحال تتمثل في إصدار الجديد من الدوريات الإلكترونية. ففي المجتمعات الحديثة، مجتمعات تكنولوجيا المعلومات، فإن الدوريات العلمية الإلكترونية التي تثبت عبر الخدمات المباشرة (electronic online journals)ليست محدودة بعدد معين من الصفحات، ولذلك فإنها تستطيع نشر مواد تجذب عدداً غير محدود من القرّاء. وفي السنوات الأخيرة، حدثت طفرة هائلة في عدد مثل هذه الدوريات العلمية والأكاديمية، وقد يؤدي هذا التكاثر إلى أن يصبح من الصعب أن نكتشف عملاً تم انتحالها لأن عدداً قليلاً من القراء سوف يعلمون إذا ما قامت دورية مشابهة بنشره في مكان آخر(١١١). ويزداد خطر تكنولوجيا المعلومات عندما يتم عبرها ارتكاب جريمة الانتحال ولا سيما عند القيام بإبرام

صفقات تجارية وبأموال طائلة تحت اسمه، مما ولّد خسارات وسرقات كبيرة يعاقب عليها القانون.

٩- جريمة السب والقذف:

تؤكد تكنولوجيا المعلومات قدرتها الكبيرة على تجاوز كل الحدود يوماً بعد آخر، بل وتؤكد كما يتخيل العديد من مستخدمي تكنولوجيا المعلومات قدرتها على الإنفلات من سيطرة الرقيب، التي طالما عرفتها المجتمعات الإنسانية منذ القدم وعانت منها كثيراً طبقات المجتمع لا سيما طبقة الكتّاب والمفكرين.

تحت الانفلات من الرقيب كثيراًَ ما تعمل بعض النفوس الضعيفة على التشهير بزملائهم أو رؤسائهم في العمل أو القادة السياسيين الدولية وتعدد أغراضهم من جراء قيامهم بذلك، فقد يكون غرضهم من ذلك التشفي أو حب الظهور وتسليط الأضواء عليهم. ويعرف القذف بأنه "القول أو الصياح علناً إذا حصل الجهر به بإحدى الوسائل الميكانيكية في محفل عام أو طريق عام أو أي مكان آخر مطروق أو إذا حصل الجهر به أو ترديده بحيث يستطيع سماعه من كل في مثل هذا الطريق أو المكان إذا أذيع بطريق اللاسلكي أو أية طريقة أخرى".

أما السبب العلني فهو "كل سب لا يشتمل على اسناد واقعة معينة، بل يتضمن بأي وجه من الوجوه خدشاً للشرف أو الاعتبار يعاقب عليه بالحبس مدة لا تتجاوز سنة وغرامة لا تقل عن ألف جنيه ولا تزيد عن خمسة آلاف جنيه أو إحدى هاتين العقوبتين".

يمكن توقيع عقوبة القذف أو السب العلني أو غير العلني أو القذف بطريق التليفون على من يقوم بإرسال شتائم إلى الغير بواسطة شبكة الانترنت، وسواء تم ذلك عن طريق إنشاء موقع خاص على شبكة الانترنت لسب أو قذف شخص معين أو سواء كان السب أو القذف عن طريق إرسال بريد إلكتروني للشخص المجنى عليه.

عليه يجب أن نميز بين عدة افتراضات وهي:

١- في حالة إسناد أموراً إلى شخص لو كانت صادقة لأوجبت عقاب من أسند إليه بالعقوبات المقررة قانوناً أو أوجبت احتقاره عند أهل وطنه وتم ذلك بواسطة شبكة الانترنت. سواء كان ذلك عن طريق إنشاء موقع على الإنترنت أو عن طريق الدخول إلى غرف الحوار، فإن ذلك الفعل يشكل جريمة قذف وذلك لتوافر عنصر القذف بالإضافة إلى عنصر العلانية، حيث إن الدخول إلى شبكة الإنترنت مباح لكافة الأفراد، من جميع سكان العالم، ولا تكاد شبكة الإنترنت أن تخلو من المتعاملين معها في أي وقت من الأوقات. كما أن شبكة

الإنترنت يمكن الحصول منها على صوت باستخدام ميكروفون، وحتى لو لم يتم الاستعانة بالميكروفون فعنصر العلانية متوافر، ويتمثل في الجهر بالقذف كتابة على الموقف المتواجد على الشبكة.

٢- وفي حالة القذف الذي يتم بإرسال بريد إلكتروني للشخص أو عن طريق المحادثة أو التحاور والذي يعرف (الجات)، فهنا إذا اعتبرنا ركن العلانية غير متوافر للخصوصية التي يتمتع بها البريد الإلكتروني، حيث لا يطلع عليه غير صاحبه فيعد هذا الفعل معاقباً عليه باعتباره جريمة قذف عن طريق التليفون؛ وذلك لأن الاتصال بشبكة الانترنت غالباً ما يتم عن طريق استخدام جهاز التليفون.

٣- أما بالنسبة للسب عن طريق استخدام شبكة الانترنت فيتحقق في حالة ما إذا تم فعل السب أثناء تواجد الشخص داخل غرف الحوار أو تم إنشاء موقع على الانترنت يتضمن أقوال تعد سباباً في حق شخص معين. فهذا الفعل يشكل جريمة سب علني لتوافر عنصر العلانية، أما في حالة السب عن طريق إرسال بريد إلكتروني لشخص يتضمن ألفاظاً وأقوالاً تعد سباباً أو المحادثة معه، فإن الفعل يعد جريمة سب غير علني لافتقاده عنصر العلانية.

من الأمثلة والشواهد على جرائم القذف والسب، حدث في مصر أن قام شاب يعمل في شركة بالجيزة بتصميم موقع إباحي على الإنترنت، وكذلك بريد إلكتروني باسم زميلته في الشركة وبدأ بإرسال صور وكلام خارج لجميع زملائهم في العمل، وعلمت زميلته بوجود موقع إلكتروني لها على شبكة الإنترنت فتقدمت بشكوى للجهات الأمنية، وبعد أن تم الكشف عن مصدر الرسائل تبين أنها من ألمانيا، لقد استغل زميلها "سيرفر" الشركة الألمانية في حين وجود الجهاز المرسل لهذا البريد المزعج في المبنى المقابل (٤٢).

١٠- جرائم التجسس وتهديد الأمن:

ظهر في مطلع الستينات من القرن العشرين مصطلحان جديدان في عالم تكنولوجيا المعلومات هما الشبكات (Network)، والهاكرز (Hackers)، كان يشار إلى الهاكرز بالمبرمجين المهرة القادرين على التعامل مع الكمبيوتر ومشكلاته بخبرة ودراسة، إذ أنهم كانوا يقدمون تطوعاً حلولاً لمشكلات البرمجة. ومن هذه الفئة ظهرت فئة أخرى تملك القدرة على فك البرامج وكسر رموزها وأرقامها السرية؛ وذلك بسبب امتلاكها لمهارات الهاكرز.

ونظراً لما سببته الفئة الأخيرة من مشكلات وخسائر لا حصر لها، فقد أطلق عليهم اسم مرادف للهاكرز وهو الكراكرز (crackers)، وهي كلمة مأخوذة من كلمة (crack) الإنجليزية

وتعني الكسر أو التحطيم، وكان الهاكرز في تلك الفترة يعتبرون عباقرة البرمجة، فهو المبرمج الذي يقوم بتصميم أقوى وأسرع البرامج والغالب في الوقت ذاته من المشكلات والعيوب.

ينقسم المحربون والمخترقون إلى قسمين هما: المحترفون والهواة، فالمحترفون عادة ما يحملون درجات جامعية عليا في مجال الكمبيوتر ويعملون محللي نظم ومبرمجين ويكونون على دراسة ببرامج التشغيل، معرفة عميقة بخباياها والثغرات الموجودة بها، بالإضافة إلى خبرة كبيرة في الشبكات.

أما الهاوي فقد يكون حاملاً درجة علمية أو لديه هواية شديدة في البرمجة ونظم التشغيل فيظل مستخدماً للبرامج والتطبيقات الجاهزة، ولكنه يطورها حسبما تقتضيه حاجته ولربما يتمكن من كسر شفراتها وبرامجها ليتم نسخها وتوزيعها بالمجال. وهذا الصنف ظهر كثيراً في الفترة الأخيرة بسبب انتشار البرامج وارتفاع أسعار برامج وتطبيقات الكمبيوتر الأصلية.

أنتجت شركة (IBM) في عام (١٩٨١) جهازاً اسمته بالكمبيوتر الشخصي (Pc) تميز بصغر حجمه وسهولة استخدامه، وبدأ الهاكرز في تلك الفترة بالعمل الحقيقي لمعرفة طريقة أداء هذه الأجهزة وكيفية تخريبها، كما ظهرت في تلك أيضاً مجموعات من الهاكرز كانت تقوم بعمليات التخريب في أجهزة المؤسسات التجارية والحكومية.

كانت لهم القدرة على اختراق أنظمة الأمان (security systems) على عكس الـ (crackers) الذين يملكون القدرة على فك شيفرات البرامج وحقوق النشر، إن الـ (Hackers) يختلفون عن الــ (crackers) على الرغم من تشابههما، فكلاهما يحاول تخطي حاجز الأمان والسرية ولكن لكليهما هدفه وأسلوبه(٤٣).

وفقاً لذلك، وفرّت تكنولوجيا المعلومات فرصة للتواصل مع الآخر، لا سيما أولئك الذين لديهم القدرة على اختراق المجال المعلوماتي أو السايبيري والإضرار به، من خلال ارتكاب جرائم عديدة ومنها جريمة التجسس والتخريب والقرصنة داخل شبكات المعلومات العالمية. وباتت المؤسسات الأمنية التي كانت في يوم من الأيام مسؤولة عن حماية الناس والدولة، بات أمنها مهدد بفعل أولئك الذين بات بإمكانهم اختراق الحدود الأمنية التي رسمتها تلك الدوائر، بل ودولها أيضاً. لقد ساعدت تكنولوجيا المعلومات العديد من الناس على ارتكاب أيضاً عدد من الجرائم وفقاً لمفهوم الجريمة في القانون ومن الجرائم التي انتشرت عبر الإنترنت جرائم التجسس على الآخرين.

كيف ترتكب جريمة التجسس؟

يمكن القول: إن ارتكاب جريمة التجسس يتم عن طريق إدخال ملف تجسس إلى المجني عليه، ويسمى هذا الملف حصان طروادة "وحصان طروادة هو الحصان الخشبي الذي استخدمه

الجيش المحاصر لطروادة كخديعة حرب، حيث لم يتمكن المهاجمون من اقتحام حصون طروادة فلجأوا إلى هذه الخديعة بأن ينسحب الجيش ويترك مكانه حصاناً خشبياً فأخذه أهل طروادة وأدخلوه الحصن ولم يعلموا أن جنود الأعداء مختبئون فيه، وعندما جنّ الليل فتحوا بوابة تتم من الداخل وقاموا بفتح البوابات في الوقت الذي عاد فيه الجيش المهاجم إلى محاصرة طروادة، وهكذا تمكنوا من الدخول والسيطرة واستباحة المدينة"(٤٤)

ينطبق الحال كذلك على حالات التجسس التي تم عبر تكنولوجيا المعلومات وتحديداً من خلال الانترنت وفي حالة إصابة الجهاز بملف التجسس يقوم على الفور بفتح أحد المنافذ في جهاز الشخص المجني عليه، وهذا هو الباب الخلفي لحدوث اتصال بين جهاز الشخص المجني عليه وجهاز المخترق. والملف الذي يكون لدى المجني عليه يسمى الخادم. بينما الجزء الآخر منه يسمى العميل وهو يكون لدى المخترق، والذي من خلاله يمكن للمخترق أن يسيطر على جهاز المجني عليه دون أن يشعر، فبإمكان المخترق فتح القرص الصلب لجهاز المجني عليه والعبث به كيفما يشاء سواء بحذف أو بإضافة ملفات جديدة. كذلك يمكن للمخترق معرفة كل كلمات السر المخزنة في الجهاز بداية من اشتراك الانترنت وحتى رقم بطاقة الإئتمان. كذلك يمكن للمخترق إذا كان لدى المجني عليه ميكروفون أو كاميرا ديب أن يستمع ويرى كل ما يفعله المجني عليه في المساحة التي يغطيها الميكروفون أو الكاميرا.

غالباً ما تكون عملية الإختراق عشوائية. بمعنى أن المخترق لا يعرف جهاز أحد الأشخاص بعينه فيقوم بإختراقه. إلا أنه من الممكن للمخترق أن يحدد جهاز مملوك لشخص معين ويقوم باختراقه؛ وذلك عن طريق معرفة رقم (الأي بي)، الخاص به لحظة اتصال الشخص بشبكة الانترنت ورقم (الأي بي) رقم ديناميكي متغير فهو رقم يتغير في كل مرة يدخل الشخص على شبكة الإنترنت.

يتم إدخال ملف التجسس إلى جهاز المجني عليه، عن طريق ثلاثة طرق:

١- إما عن طريق برامج المحادثة، حيث يقوم المخترق بإرسال ملف للمجني عليه ويؤكد له أنه يحتوي على لعب مثيرة أو غير ذلك من الإغراءات، فينخدع المجني عليه ويقوم باستقبال الملف.

٢- وإما تكون عن طريق البريق الإلكتروني، حيث يقوم المخترق بإرسال رسالة إلى المجني عليه فيقوم بفتحها، فإذا به يحتوي على ملفات ملحقة تحمل برنامج الاختراق.

٣- أو تكون عند زيارة الشخص لمواقع مجهولة تغريه بتنزيل بعض البرامج والملفات المجانية ومن ضمنها ملف التجسس (٤٥).

ما وسائل الاختراق؟

هناك عدة وسائل لاختراق (Penetrat) الأجهزة، ويمكن عمل ذلك من خلال الثغرات الأمنيـة أو رقـم الـ (IP) أو الـ (Port) أو الـ (Cookies)، ويمكن تصنيف طرق الاختراق إلى ثلاث طرق:

١- اختراق الأجهزة الرئيسي للشركات والمؤسسات من خلال تخطي الجدران النارية (Fire wall)، كما حدث في اختراق برنامج الـ (Hotmail) الخاص بالبريد الإلكتروني، وغالباً ما يتم ذلك باستخدام المحاكاة والخداع (Spooring)، وتستخدم هذه الطريقة لانتحال شخصية ما لخداع الأنظمة والدخول عليها. ويتم استخدام طريقتين لعمل ذلك، الطريقة الأولى باستخدام عنوان الـ (IP) الذي يحتوي بدوره على بيانات المرسل والمرسل إليه، والطريقة الثانية، من خلال مسارات المصدر (Routing source)، إذ أن حزم الـ (HP) تم إعطاءها شكلاً تبدو معه وكأنها قادمة من كمبيوتر معين موثوق به، بينما هي في حقيقة الأمر هي ليست كذلك.

٢- اختراق الأجهزة الشخصية، وهي مـن أكـثر الطـرق شـيوعاً، ويـستخدم في ذلـك عنـوان الــ (IP) ورقـم (Port)، و (Protocol).

٣- التعرض لحزم البيانات (Packets) أثناء انتقالها وفك شفراتها (Decrypt) وتستخدم هذه الطريقـة لكـشف أرقـام بطاقات الإئتمان (Credit cards) والأرقام السرية للبطاقات البنكية (ATM)(٤٦).

كيف تتم ميكانيكية الاختراق؟

يعتمد الاختراق على السيطرة عن بعد (Remotely)، وهي لا تتم إلا بوجود عاملين مهمين : الأول البرنـامج المـسيطر ويعرف بالعميل (Client)، والثاني الخادم (Server) الذي يقوم بتسهيل عملية الاختراق ذاتها.

تختلف طرق اختراق توافر اتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم الخاص بالمخترق، وجهاز المخـترق على الطرق الآخر، حيث يوجد برنامج المستفيد أو العميل. وهناك ثلاث طرف شائعة لتنفيذ ذلك، نذكر منها طريقة ملفـات أحصنة طروادة (Trojan) السابقة الذكر، ولتحقيق نظرية الاختراق لا بد من توافر برنامج تجسسي يتم إرسـاله وزرعـه مـن قبل المستفيد في جهاز الضحية ويعرف "الملف اللاصـق أو الـساكن" وهـو ملـف (Patch) صـغير الحجـم ومهمتـه الأساسـية التجسس على جهاز الضحية، ويعتبر هذا البرنامج حلقة الوصل بين المخترق والضحية. ويتم زرعه بجهازك عن طريق المخترق وذلك بإرساله إليك عن طريق الخطأ بسبب عبثك في برامج الاختراق.

حيث يدخل الملف لجهاز الضحية يغير من هيئته وموقعه: لهذا السبب تكمن خطورة أحصنة طروادة فهي من جانب تدخل الأجهزة في صمت وهدوء، ويصعب اكتشافها، من جانب آخر حتى في حالة وجود برنامج جيد مضاد للفيروسات. ولا تعتبر أحصنة طروادة فيروسات وإن كانت برامج مضادات الفيروسات تعتبرها كذلك ، فهي بالمقام الأول ملفات تجسس، ويمكن أن يسيطر من خلالها المستفيد سيطرة كاملة على جهاز الضحية عن بعد، وتمكن خطورتها في كونها لا تصدر أية علامات تدل على وجودها بجهاز الضحية. وتتم عملية إرسال ملفات التجسس بعدة طرق من أشهرها البريد الإلكتروني(٤٧).

تعد تلك الخروقات التجسسية جرائماً ترتكب بحق الأفراد والدول، وبالتالي باتت المجتمعات تمسي وتصبح على العشرات من هذه الجرائم التي تتم عبر تكنولوجيا المعلومات. وتزداد القناعة يوماً بعد يوم بإمكانية الاستخدام السلبي لشبكات المعلومات من جانب العناصر الهدامة للمجتمع. فقد اكتشفت الجهات الأمنية في المجتمعات المستخدمة لشبكة الانترنت رسائل مشفرة، تتصل بتهريب المخدرات والحث على التخريب والعنف من قبل المتطرفين والمنفذين للحروب الأهلية، وقد أكدت عملية الانفجار الرهيب الذي شهدته مدينة أو كلاهما الأمريكية هذه المخاوف.

تعد أعمال التجسس من أخطر السلبيات لهذه الشبكات العالمية، فقد أصبح البنتاجون أو وزارة الدفاع الأمريكية تخشى هجمة مماثلة لهجمة "بيرك هاربور"، (Perai Harbor)، التي تعرضت لها في أثناء الحرب العالمية الثانية من قبل اليابان، بيد أن الهدف هذه المرة لن يكون الأسطول الأمريكي، وإنما أجهزة الكمبيوتر التابعة لهيئة الأركان، والتي بلغ عددها حوالي (١٥٠) ألف جهاز.

أرادت هيئة الأركان الأمريكية التحقق من مدى مناعة تجهيزاتها، فأوكلت إلى فريق من القراصنة العسكريين مهمة، اختراق شبكة البنتاجون، ومحاولة النفاذ إلى قواعد معلوماتها عبر شبكة الانترنت وغيرها من شبكات المعلومات . والنتيجة المذهلة كانت توصل الفريق إلى الإحاطة بمضمون (٨٠%) من أجهزة الكمبيوتر الرئيسة، وأن جهاز الحراسة والمراقبة لم يفطن من جانبه إلى أن (٤%) فقط من الحالات.

يدلل ذلك، بل ويؤكد على حقيقة مفادها: سهولة اختراق شبكة وزارة الدفاع الأمريكية، أن هذه الشبكة قد تعرضت للاختراق أكثر من (٣٠٠) مرة خلال عام (١٩٩٤). ولذا... فإن الولايات المتحدة غير مهيأة لمواجهة هجوم إلكتروني؛ لأن مناعتها غير موفقة في هذا المجال حتى اليوم (٤٨).

وإذا كان الأمر هكذا بالنسبة للولايات المتحدة الأمريكية مخترقة شبكة الإنترنت، وكذلك توفر الإمكانيات التقنية العالمية ووجود الكوادر البشرية المتطورة فنياً من الناحية التقنية واخترقت وزارة دفاعها، فما بالك بالنسبة للدول الأخرى وكذلك الأفراد؟!

١١- جريمة المساعدة على الانتحار:

يبدو من خلال النظر إلى الواقع الاجتماعي للحياة، ومن ثم رصد الواقع الفعلي لتطبيقات تكنولوجيا المعلومات، أنها طالت جميع نواحي الحياة، الإيجابي منها والسلبي على حدٍ سواء. ففي الجوانب السلبية يمكن القول: إن كل من ارتكب أو قام بفعل إجرامي أو ساعد على ارتكاب فعل إجرامي فهو مجرم من وجهة نظر القانون. ومن هنا نلحظ من خلال الدراسات التي تشير إليها مصادر المعلومات، أن خدمات تكنولوجيا المعلومات، لا سيما خدمات الانترنت اتسعت لتغطي أغلب مجالات الحياة، ومنها الجانب السلبي، ولكن أغرب هذه الخدمات ما تقدمه اليابان عبر الشبكة، حيث وفرت شبكة الإنترنت خدمة خاصة للانتخار، لتسهيل عملية قتل النفس لكل من يرغب في ذلك، نظير دفع المقابل المادي لذلك بالطبع. وقد ساعدت هذه الخدمة امرأة واحدة على الأقل في الإقدام على الانتحار، كما أرسلت سبعة طرود بريدية من أقراص سيانيد البوتاسيوم القاتلة لسبعة أشخاص طلبوها عن طريق الانترنت.

اكتشف البوليس الياباني هذا الموقع في (١٥) ديسمبر (١٩٩٨)، وقد تبين أن الشخص الذي يديره صيدلي يمتلك ترخيصاً بمزاولة المهنة. وكان البوليس يبحث عن شخصين طلباً كبسولات سيانيد للبوتاسيوم، في طريق الموقع، الذي كتب فيه باللغة اليابانية أنه مخصص للأشخاص الذين لا يعرفون طريقة الحصول على العقار الصحيح للانتحار (٤٩).

وقد حدث مرة القتل العمد بطريق الإنترنت حين قام أحدهم بقتل زوجته والتي كانت موضوعة تحت جهاز (monitoring)، عندما دخل عن طريق الإنترنت إلى الشبكة الداخلية للمستشفى وغيّر في الوصفات الطبية الخاصة بها على نحو قاتل، وحين أعطيت الأدوية من قبل المرضة - التي عدّت بمثابة وسيلة مادية لا قصد لديها - ماتت المريضة*؛ ولمعرفة المزيد عن هذا النوع من جرائم تكنولوجيا المعلومات ما علينا سوى الصبر والانتظار.

وستبدي لك الأيام ما كنت جاهلاً   وتأتيك بالأخبار ما لم تزود

١٢- جرائم الجنس والعِرْض عبر الإنترنت:

لقد جرت العادة في سائر المجتمعات، وبينها المجتمع العربي والإسلامي، استقبال كل زائر جديد بالفرح والإنتاج؛ لأن هذا الضيف القادم له وقع وأثر على نفس الضيف، وقد يرحل هذا الضيف بعد فترة وجيزة، وقد يمكث مع أفراد الأسرة ويصبح واحداً منهم، بل جزءاً من العائلة، وربما يكون الضيف الجديد ليس إنساناً، بل آلة أو حيواناً أليفاً أو ما شابه ذلك. والجميع يتذكر كيف كان لوقع التلفاز من أثر إيجابي ولا زال في حياة الأسرة، وأصبح لا يمكن الاستغناء عنه

داخل البيت مهما كان مستوى الأسرة الاقتصادي ومن بعد ذلك جاءت تكنولوجيا المعلومات تباعاً بوصفها ضيوفاً في بادئ الأمر، ومن ثم أضحت فرداً من أفراد الأسرة والمجتمع.

شبكة الإنترنت هي الضيف أو الزائر القادم من داخل وخارج أسوار الموقع الجغرافي للبيت وللدولة، زارنا دون مقدمات، وأصبح حاضراً ليس في الحالات الهامة فحسب، بل داخل البيوت، لا بل وداخل غرف نومنا، وغرف أطفالنا بوصفه أنيساً لهم وفي ذات الآن يعلمهم ويوسع في آفاقهم بعيداً عن غرف الدراسة والمعلم، ولا شك في ذلك ما للإنترنت من وجه مشرق أضاء دهاليز الظلام في دروبنا وقبلتها عقولنا، وأحاطنا علماً في العديد من الأشياء، والأحداث العلمية وغير العلمية التي تقع خارج أسوار وطننا، وأصبحت النافذة التي تظل عبرها إلى الآخر أينما كان وفي أي زمان. بيد أن السؤال المهم هنا مفاده: هل ينبغي النظر إلى هذا الوجه المشرق والمضيء ونحجب الرؤيا عن الجوانب الأخرى؟ بمعنى آخر هل هناك جانب سلبي في عالم الإنترنت فيه خطورة على الصغار أكثر من الكبار؟ والإجابة عن ذلك تأتي بكل تأكيد بـ (نعم) فمثلما الإنترنت جوانب إيجابية فلها جوانب سلبية، وهذه سنة الحياة.

الوجه السلبي للإنترنت يمكن أن ترتكب عبره جرائم الجنس يتمثل في وجود مواقع على شبكة الإنترنت تحرض على ممارسة الجنس سواء مع الكبار أو مع الأطفال. وتقوم هذه المواقع بنشر صور جنسية فاضحة للبالغين والأطفال. وإذا كانت الدعوى لممارسة الجنس الموجه للبالغين يمكن أن تلاقى بالرفض أو القبول وذلك لتوافر تمام العقل لدى البالغين، فإن الوضع بالنسبة للطفل يختلف وذلك لصغر سنه، وعدم اكتمال نضجه العقلي. لذلك فالطفل أكثر عرضة للإنخداع بهذه المشاهد والصور الجنسية الساخنة، ويتم استخدام التكنولوجيا الحديثة في هذه الصور عن طريق تركيب رؤوس أشخاص معروفين كالفنانين على أجسام أشخاص آخرين(٥٠).

بيد أن المشكلة تتفاقم أكثر وأكثر عندما تتعلق بالأطفال الذين يستطيعون الوصول إلى المحادثات الجنسية (Sexual Conversation)، ويتبادلون صور المعاشرة الجنسية (hardcore pictures)، أو يصادفون مراهقين يغرونهم بمقابلتهم ، كذلك فأحياناً قد تبدو الرسالة كأنها مرسلة من فتاة تبلغ اثنى عشر عاماً، في حين أنها قد تكون مرسلة في الحقيقة من رجل في الثلاثين من عمره. وهكذا، يجب أن يتم تحذير الأطفال بألا يقوموا مطلقاً بإفشاء معلومات شخصية، فأن يخبروا آباءهم إذا ما تلقوا بريداً إلكترونياً أو رسائل تجعلهم يشعرون بعدم الراحة (٥١).

أضف على ذلك، فإن شبكة الإنترنت يزداد أثرها سوءاً على الأطفال من خلال نقل هذه الشبكة إلى الأحداث - ثقافة الإباحية- حيث تتضمن هذه الشبكة حوالي مليون صورة أو رواية

أو وصف، وكل هذه الأشياء لها علاقة مباشرة وما صنعته بالجنس، إضافة إلى ذلك فإن الشبكة توفر معلومات واضحة حول بيوت الدعارة والعاهرات في العديد من دول العالم.

أما بالنسبة لجرائم العرض وإفساد الأخلاق للأحداث فيمكن الشخص في سلوكه الجنسي ما يبعده عن أي لوم يوجه إليه من المجتمع، ولذلك لتحدد العرض وفقاً لمجموعة من القيم الاجتماعية ذات مصدر ديني وأخلاقي في الغالب.

بيد أن (العرض) من الناحية القانونية يعني - الحرية الجنسية - ولذلك يعد الفعل اعتداءً على العرض متى تضمن الاعتداء على الحرية الجنسية للشخص، كأن يكره الشخص آخر على مسلك جنسي معين، أو يتضمن الفعل خروجاً على الحدود التي وضعها القانون على هذه الحرية.

أما بخصوص أثر الإنترنت على اقتراف الحدث سلباً أو إيجاباً مثل هذه النوعية من الجرائم وهي جرائم العرض وإفساد الأخلاق على الحدث، فإن تلك الجرائم تصنف على أنها جرائم تقوم على الاتصال الجسدي بالقاصر مثل جرائم الاغتصاب أو اعتداءات جنسية أخرى لا تعد اغتصاباً، وهناك اعتداءات جنسية دون عنف وهو يعني كل فعل فاحش أو فاجر يقع على الحدث، ولكن دون عنف أو اكراه أو تهديد أو مباغتة. وقد تتمثل هذه الجريمة في إتيان أفعال فاحشة أو مخلة بالحياء في حضور فتاة صغيرة، الأمر الذي يؤدي بدورها أن تستسلم لأعمال البغاء أو الدعارة، وكذلك تأجير غرفة للصغار يمارسون فيها أعمال الفجور أو الفسق، وممارسة العادة السرية أمام صبي أو صغير عمره (١٦) سنة.

والحقيقة يتصور وقوع أفعال حض الطفل أو القاصر على الانحراف الجنسي من خلال شبكة الإنترنت التي تعد بمثابة غاية للقصر محدودي المعرفة، ومن المواد غير المرغوب فيها الصور أو المشاهد الإباحية والإعلانات التي تعدم القيم لدى الطفل.

علاوة على ما سبق، يمكن إفساد القاصر أو دفعه للانحراف من خلال اشتراكه في منتديات الحوار أو غرف الدردشة، وكذلك البريد الإلكتروني والقوائم الإلكترونية؛ وذلك من خلال المعلومات الجنسية المغلوطة أو المقرصة التي يتلقاها دون رقيب أو يسوء فيه، ممن يتولى مخاطبته أو تزويده بهذه المعلومات لا سيما عن طريق القوائم الإلكترونية.

يبقى بعد ذلك كله سؤالاً مهماً مفاده: ترى ما الذي يدفع هؤلاء إلى الاتصال بمثل هذه المواقع، ومن ثم يدعوهم إلى ارتكاب جرائم جنسية؟

الإجابة عن هذا السؤال جاء من خلال دراسة أجراها مركز أبحاث - في أحدث الدول العربية - عن المواد الإباحية التي تبث عبر الشبكة) وذلك من خلال استبيان تم توزيعه عبر شبكة الإنترنت، وأسفرت هذه الدراسة عن:

١- (٤٨%) من الذين شملتهم الدراسة يرون عدم فرض قيود على المواد المتاحة.

٢- (١٨%) ممن شملتهم الدراسة، سعوا لمعرفة المواد الإباحية المتاحة.

٣- (٩٥%) ممن شملهم البحث، سعوا إلى الوصول للمواد الإباحية، ولم يجدوا صعوبة في عملية الوصول (٥٢).

١٣- جريمة غسيل للأموال عبر الإنترنت:

تعد جريمة غسيل الأموال هي من الجرائم المعاصرة، وهي صورة من صور الجريمة المنظمة. ولقد استخدمت تكنولوجياً المعلومات الحديثة بوصفها واحدة من الأساليب الجديدة في غسيل الأموال.

لقد كان متعارفاً لدى الناس أن غسيل الأموال يتم عن طريق بعض الأساليب التقليدية، بيد أن الأمر يكاد يكون مختلف تماماً عن سابقه، إذا أصبح من الممكن أن تتم عملية غسيل الأموال عن طريق أساليب مستحدثة تتوائم مع طبيعة العصر ومستحدثاته. ومن الآثار السلبية لاستخدام الإنترنت، استخدامها في غسيل الأموال عن طريق تحويل الأموال أو توظيفها والتعامل مع البنوك عبر الإنترنت أو إجراء عمليات معقدة من التحويلات النقدية من حساب لآخر لإخفاء الصفة غير المشروعة لمصدر الأموال القذرة. فيكفي إعطاء أمر عبر الإنترنت لتفتح أمامك نوافذ وآفاق متعددة للتجارة الإلكترونية وللبيع والشراء والتعاقد واكتساب الحيازة والممتلكات والتحويلات بلا قيود، ما يشكل بعض صور الركن المادي لجريمة الغسيل (٥٣). وفعل انتقال الأموال من منطقة جغرافية إلى أخرى عبر الإنترنت يعد واحداً من الوجوه السلبية للإنترنت، لا سيما الأموال التي جاءت عن طرق غير شرعية.

تكنولوجيا المعلومات وعولمة الجريمة:

بات مؤكداً أن تكنولوجيا المعلومات لعبت دوراً مهماً في تقريب الناس بعضهم إلى بعض، وبالفعل عملت ليس على اسقاط الحدود والمسافات بين الدول، بل عملت على إسقاط الجدران بين الناس، وها هم المنادون بالحرية والديمقراطية يرفعون شعارات من ضمنها: فلتسقط تلك الجدران ويعيش الناس بلا حدود، بلا قيود، إنها نهاية الجغرافية.

يلاحظ المتتبعون للثورة التكنولوجية الحديثة والثورة المعلوماتية التي حررت الإنسان من قيود الزمان والمكان، وظهور النظام العالمي الجديد والذي تسيطر عليه قوة عظمى وحيدة في العالم هي الولايات المتحدة الأمريكية، أصبحت هناك عولمة ثقافية واقتصادية وعولمة اتصالات وغيرها.

وكلها مؤشرات على بداية تكوين مجتمع عالمي واحد، وهذا السوق العالمي أدى إلى أن تتجه عصابات الجريمة المنظمة إلى العولمة كذلك، ومن ثم فقد اتسع نطاق الجريمة ليخرج من النطاق الإقليمي إلى النطاق الدولي، فوجدت الجرائم - عابرة الحدود أو عابرة القارات - وظهرت الجرائم المستحدثة، مثل الجريمة المنظمة الحديثة عابرة الحدود والجريمة المعلوماتية عابرة القارات، والجرائم الاقتصادية كالاحتيال من خلال التسوق عن بُعد وتحويل الأموال إلكترونياً وغسيل الأموال(٥٤).

تتم الآن كل تلك الجرائم السابقة الذكر عن طريق تكنولوجيا المعلومات، وهذه التكنولوجيا هي التي حققت ما يسمى بالقرية الكونية التي أشار إليها العالم مارشال ماكلوهان، وطالما تحققت تلك النبوءة بات العالم يعرف ما يدور هنا وهناك في الأماكن القريبة والبعيدة على حد سواء، وأصبح العالم يعيش لحظة مشتركة لحدث ما أو فعل ما، بمعنى آخر، إنها عولمة الأشياء والأفعال بخيرها وشرها، وذلك كله تحقق بفضل تكنولوجيا المعلومات وتحديداً الانترنت.

كيف تستخدم الإنترنت في جريمة غسيل الأموال؟

يمكن تعريف جريمة غسيل الأموال بأنها "مجموعة العمليات المالية المتداخلة لإخفاء المصدر غير المشروع للأموال، وإظهارها في صورة أموال متحصلة من مصدر مشروع أو المساهمة في توظيف أو إخفاء أو تحويل العائد المباشر لجناية أو جنحة" كذلك عرفت اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمبرمة في فينا (١٩٨٨)(، وقد نصت الاتفاقية على صور ثلاث لغسيل الأموال تتمثل في "تحويل الأموال أو نقلها مع العلم بأنها مستمدة من جرائم المخدرات، إخفاء أو تمويه حقيقة الأموال أو مصدرها، واكتساب أو حيازة أو استخدام الأموال مع العلم وقت تسليمها بأنها مستمدة من جريمة من الجرائم المنصوص عليها في الاتفاقية"(٥٥)بناءً على ما تقدم، فإن جريمة غسيل الأموال هي جريمة تابعة تفترض ابتداءً سبق ارتكاب جريمة أولية نتج عنها أموال غير مشروعة، ثم تأتي في مرحلة تالية عملية غسيل تلك الأموال القذرة لتطهيرها في إحدى صور الغسيل، ولكن لإرتكاب إحدى صور السلوك الإجرامي المكون لجريمة غسيل الأموال يفترض وجود محل الجريمة، وهو المال الذي يتم غسله بعد تحصيله من مصدر غير مشروع، وذلك كركن مفترض للجريمة(٥٦).

عملية الغسل عبارة عن توظيف هذه الأموال داخل الدولة أو خارجها في أعمال مشروعة لطمس الأصل غير المشروع لهذه الأموال، وذلك من خلال تسلل هذه الأموال إلى المشروعات الاقتصادية

والتأثير فيها، وبذلك تمّر الأموال المتحصل عليها من جرائم خلال قنوات استثمار شرعية، ويعاد استغلالها بعد ذلك على أنها من مصدر ربح مشروع، وتغسل هذه الأموال بواسطة بعض البنوك والمصارف والشركات متعددة الجنسيات بهدف الربح وإخفاء حقيقة مصدرها، وللمزيد من التضليل يقوم أشخاص آخرون غير أعضاء المنظمة بغسل هذه الأموال مقابل مبالغ نقدية تدفع لهم لعدم كشف مصدرها الحقيقي.

تشمل عملية غسل الأموال القذرة الناتجة من أنشطة إجرامية غير مشروعة كالاتجار في المخدرات وعمليات تهريب الذهب والأحجار الكريمة، والتهرب من الضرائب، والاتجار في الأعضاء البشرية والنساء والأطفال، وإدارة شبكات الدعارة، والاتجار غير المشروع في الأسلحة والمواد النووية والابتزاز وتزييف وتزوير العملات وغيرها من الجرائم المنظمة المعاصرة.

فالجريمة الاقتصادية المنظمة، بما فيها غسيل الأموال، يلجأ مرتكبوها إلى استخدام التقنية الحديثة في ارتكاب جرائمه، وتقام شركات مشروعة ليتستر خلفها ويرتكب أنشطة غير مشروعة دون أن يدري عنه أحد شيئاً وهو أسلوب للتمويه حال ارتكاب الجرائم الاقتصادية.

أما استخدام الانترنت في غسيل الأموال له وجوه عديدة، من ذلك استخدام بطاقة الائتمان لشراء مجوهرات يتم سداد الفاتورة الخاصة بها فيما بعد، بالنقد العائد من عملية الاتجار في المخدرات، كذلك يمكن استخدام بطاقات الائتمان المسروقة لشراء أشياء ثمينة، ويصف أحد الباحثين العلاقة بين الإنترنت وغسيل الأموال: بأنها حركة سريعة ولا توقفها الحدود الجغرافية، والجودة ذاتها تجعل الإنترنت والبطاقات الذكية محل ترحيب من الجمهور، وكذلك محل جاذبية من المجرمين الذين هم في شوق لغسل أموالهم بهدوء وسرعة، فالنقود الإلكترونية، وسيلة سهلة في التحويل والنقل من مكان لآخر.

يكفي للتدليل على خطورة البطاقات الذكية (Smart cards) والتي يمكن عن طريقهما تحويل النقود بطريق الانترنت ولا سيما في مجال غسيل الأموال، الإشارة على تقنية موندكس (m ondex) الشهيرة، ضمن تقنيات البطاقة المذكورة، حيث إن المجرمين في عمليات غسيل الأموال يمكنهم تحويل أموالهم مع تشفير عملية التحويل عبر جهاز - مودم - أو عبر الإنترنت، وبالتالي لا يمكن تتبعه أو معرفة مضمون العملية، ولذلك يجب الاعتراف بأن غاسلي الأموال أذكياء وبارعون، ولذلك فالمستقبل من الناحية - المعلوماتية - يحمل إمكانية قيام هؤلاء بعمليات غسيل الأموال بسرعة أكبر، ودون آثار تترك خلف هؤلاء والحقيقة أن الاحتيال باستخدام بطاقات الدفع الإلكتروني عن طريق شبكة الإنترنت من الجرائم الدارجة في الوقت الحالي لاستخدام هذه الشبكة في التجارة الإلكترونية، وسداد مقابل سلعة أو الخدمة بطريقة إلكترونية.

تعطي بطاقة الدفع الإلكتروني للعميل، الحق في الحصول على السلع والخدمات بإحدى طريقتين، الأولى هي الحصول على السلع والخدمات في حضور العميل، وفي هذه الحالة يحصل التاجر على بصمة بطاقة العميل مطبوعة على إشعار البيع، سواء من خلال الماكينة اليدوية أو الماكينة الإلكترونية، وتسمى هذه العملية (Face to face Hanction) أما الطريقة الثانية وفيها يحصل العميل على السلع والخدمات بموجب تصريح كتابي أو تلفوني بخصم القيمة على حساب بطاقة الدفع الإلكترونية الخاصة به وهذه الطريقة تسمى (email, phone order) وفي الطريقة الثانية، تستخدم شبكة الإنترنت في الحصول على السلع والخدمات، وسداد الثمن، ويكفي لشراء السلعة أو الحصول على الخدمة، أن يدخل العميل إلى مركز التسوق الافتراضي، ويختار السلعة التي يرغبها أو الخدمة التي يريدها، ويظهر له نموذج يقوم بملئ البيانات الخاصة ببطاقة الإئتمان التي يملكها، وعنوانه، ثم يقوم مركز التسوق الافتراضي بخصم قيمة السلعة من بطاقة الدفع الإلكتروني وإرسالها إلى عنوان المشتري.

بيد أن المشكلة التي تظهر وراء هذا النوع من البطاقات، أن بعض البنوك اكتشفت تكرار اعتراض بعض حاملي بطاقات الدفع الإلكتورني على عمليات لم يقوموا بإجرائها، وتبين للبنوك أنها عمليات أجريت عن طريق شبكة الإنترنت، حيث قام الهواة أو القراصنة بالتقاط هذه الأرقام - وذلك من الناحية الفنية أمر سهل بالنسبة لهم - واستخدام أرقام البطاقات في الحصول على السلع التي يرغبونها، وخصمت القيمة من حساب الحامل الشرعي للبطاقة .

نخلص من كل ما تقدم إلى أن عمليات غسيل الأموال بطريق الإنترنت، هي أمر وارد في ظل نمو وازدهار التجارة الإلكترونية، وذلك عن طريق تحويل الأموال أو توظيفها والتعامل مع البنوك عبر الإنترنت أو إجراء عمليات معقدة من التحويلات النقدية من حساب لآخر ومن بنك لآخر، وذلك لإخفاء الصفة غير المشروعة للأموال، وكل ذلك يتم عن طريق التجارة الإلكترونية بطريق الإنترنت(٥٧)، وهناك العديد من الأمثلة عن هذه الجريمة (جريمة غسيل الأموال) ولا يسع المجال لذكرها هنا.

١٤- جريمة تعاطي المخدرات عبر الإنترنت:

لقد بات معروفاً في أوساط المجتمع الإنساني، إن زمن الدولة وسيطرتها على حدودها وأبنائها، قد انفلت من سيطرتها، وأصبحت الحدود الشكلية هي ربما تحت السيطرة التقليدية للدولة الوطنية، وعملية الإنقلاب تلك جاءت في ظل عصر العولمة الذي تقود قافلته تكنولوجيا المعلومات ولقد كشفت الأخيرة عن عورات الدولة الوطنية التي طالما حلمت كثيراً في التستر على كل

العيوب التي تدور في الفلك الداخلي، بيد أن كل تلك الجهود باءت بالفشل، وأن التأكيد على مبادئ الدولة الوطنية قد ولى في عصر العولمة، وأن التحكم على المستوى الوطني أصبح عديم الفاعلية في ظل عصر تكنولوجيا المعلومات، والعمليات الاجتماعية والاقتصادية.. التي تدور في رحاها تتمثل عملية التشظي والانفلات من سيطرة الدولة في نقاط الحدود في السابق كانت تتجسد لقوة الدولة الوطنية في السيطرة على الحدود سواء البرية منها أم الجوية أم البحرية، أما الآن فالحدود لم تعد كما كانت تمنع وتنتقي الداخل والخارج منها، ولم تعد تعمل كمصفاة للداخلين والخارجين، المرغوبين والمطلوبين للدولة أو بين الأصدقاء والأعداء، فهذه الجماعات الأهلية العابرة للحدود مثل أطباء بلا حدود، وجماعة السلام الأخضر وغيرها، وجماعات حقوق الإنسان تجبر الدول على فتح سجونها ومعتلاقتها للتحقيق، وتشترط معونات اقتصادية، وأحياناً تعلق عضويتها في المجالس الدولية الهامة بسجل حقوق الإنسان فيها(٥٩). وبذلك تظل الدولة الوطنية تحت تهديدات خارجية يمكن أن تعرضها للإنتهاك الخارجي والمواثيق الدولية. وفي ظل تلك المعطيات أضحت تكنولوجيا المعلومات، ومنها الإنترنت واحدة من أهم الوسائل التي باتت تخترق الدولة الوطنية صباحاً ومساءً، بل وفي كل حين ومن ضمن تلك الاختراقات والتهديدات هو نقل الجريمة من الخارج إلى الداخل، ومن ضمن تلك الجرائم جريمة تعاطي المخدرات عبر الإنترنت.

أسباب تعاطي المخدرات:

قبل الخوض في حيثيات جريمة تعاطي المخدرات، ومن ثم البحث عن الحلول للحد من تلك الجريمة، كان لا بد من البحث عن الأسباب والعوامل التي تدفع بعض الناس إلى تعاطي المخدرات، ويمكن أن ندرج تلك الأسباب بالشكل الآتي:

١- الفشل الدراسي وتشغيل الشباب غير المؤهل علمياً، وبالتالي لا يمكن له التوافق مع عمله الجديد، الأمر الذي يؤثر سلباً على حياته الشخصية واليومية.

٢- صعوبة التوافق مع مجتمع تتعدد فيه الجنسيات الأخرى والقادمة من بيئات لا تتوافق وعادات وتقاليد المجتمع الأصل كما هو الحال في مجتمعات دول الخليج العربي. (وجود جنسيات هندية وباكستانية وفلبينية..)

٣- أسباب أسرية ومنها الطلاق والانفصال بين الوالدين، ووفاة أحدهما، والشعور بالحرمان الأبوي، وعدم الرقابة الأسرية لسلوك الطفل. وتتشابه المجتمعات كافة في هذا العامل.

٤- أمية الوالدين وجهلهما، وتدليل الأطفال على نحو مبالغ فيه، وتشديد الرقابة عليهم، نحو مبالغ فيه كذلك.

٥- توجه الصغار مبكرين إلى ميدان العمل لسداد احتياجات الأسرة، يؤثر سلباً عليهم فيما يتعلق بتعاطي وادمان المخدرات.

٦- الفشل الدراسي المبكر وهجر الدراسة في الصغر، وصعوبة الحصول على عمل مناسب، ومن ثم صعوبة الحصول على الاحتياجات الأساسية كالمساكن والسيارات والزواج.

٧- تدهور العلاقات والروابط الأسرية وهجر الدراسة في الصغر وانشغال الوالدين عن أولادهم بالعمل خارج المنزل أو بسبب الارتباطات العائلية.

كيف تستخدم الإنترنت في تعاطي المخدرات؟

لقد ألقت جريمة تعاطي المخدرات بظلالها على العديد من المجتمعات الإنسانية، وعانت بعض المجتمعات كثيراً في التصدي لتلك الجريمة، ومحاولة الحد من الطرق التقليدية التي تتبع في تناولها وثم انتشارها، وما أن نجحت بعض الدول في العديد من المحاولات وفشلت في الأخرى، إلا وظهرت طريقة جديدة لم تكن في الحسبان لدى بعض الدول، لا سيما الدول النامية منها، وبات من حق الجميع أن يعرف الطريقة الجديدة من خلال الإجابة عن سؤال مهم مفاده: ما الآلية التي ترتكب فيها جريمة تعاطي المخدرات من خلال الإنترنت؟

تعد الإنترنت من أهم الأدوات التي حققت حلما "مارشال ماكلوهان" عالم الاتصالات الكندي، الذي قال بأن العالم سيصبح عبارة عن قرية كونية، لكن هذا الكلام كان ينطبق على عنصر الكهرباء. إن شبكة الإنترنت العالمية يمكن من خلالها أن يكتشف الأحداث والشباب رجالاً ونساءً كيفية الحصول على المخدرات، وكيفية تعاطيها واستنشاقها سواء كانت هيروين أو كوكايين، وأن يتعرف على أماكن توزيع مخدر - الماريجوانا - وأسعاره، وكذلك المخدرات الكيماوية المصنعة مثل مخدر - الميتافيتامين - وهو منشط كيماوي معروف ومنتشر.

تعد عملية تعاطي المخدرات عن طريق الإنترنت من الصور السلبية لاستخدام هذه الشبكة، وتعكس صورة للجريمة في عالم متغير، نتيجة التغير التكنولوجي الذي طرأ على العالم وأدى إلى ظهور أنماط جديدة من الجرائم، الأمر الذي يهدد مبدأ الشرعية ومن ثم التأثير بشكل أو بآخر على حقوق الإنسان.

يلاحظ أن غرف الدردشة التي تنتشر على شبكة من الروافد التي تغذي ثقافة تعاطي وادمان المخدرات عن طريق هذه الشبكة، فعن طريق المحادثات في هذه الغرف يمكن معرفة أساليب زراعة الماريجوانا ومعالجتها وتعاطيها، بل يمكن صناعتها منزلياً عن طريق المعلومات الموجودة في بعض المواقع بمواد بسيطة وأولية موجودة في بلدان عديدة، إذ يمكن تصنيعها من الموز والفول

السوداني، ولذلك يقول أحد المسؤولين المختصين في مكافحة المخدرات من العاملين في البيت الأبيض الأمريكي: إن ما تقوم به شبكة الإنترنت العالمية، يقوض الجهود والسياسات التي تبذلها الحكومة لمكافحة المخدرات؛ وذلك لأن الشبكة تنشر معلومات تؤدي إلى زرع بذور معاداة قوانين المخدرات.

أضف إلى ما سبق أن المشكلة المترتبة على تبادل الحديث في غرف الدردشة عبر الإنترنت سلبية على الأقل من زاويتين هما: الأول: إن أولياء الأمور من وزراء وآباء ومعلمون وتربويون وغيرهم ليس لديهم كمية المعلومات الموجودة على شبكة الإنترنت؛ وذلك لأن ثقافة الحاسب الآلي لدى هؤلاء هي أقل من تلك التي توجد لدى أبناءهم الذين لديهم شغف بالمعرفة المعلوماتية، وهم أكثر قدرة ومهارة من غيرهم في تعلم مهارات الحاسب الآلي.

الثانية: إن طبيعة الحديث في غرف الدردشة عبارة عن حديث عادي بين المشاركين وتتناول فيه معلومات تتعلق بأي شيء بما فيها المخدرات، وفي حالة الإدلاء بأحاديث تتعلق بهذا الخصوص، يسهل التقاطها من قبل صبي مشارك في هذه الدردشة، ومن ثم تنتقل إليه ثقافة التعاطي والإدمان للمخدرات، فقد قال أحدهم: وهو طالب أمريكي، في المرحلة الثانوية في رحلته مع أحد عقار المخدرات: "كان أروع ما عملته"، وقال آخر في حديثه عن الجريمة الأولى من الكوكايين: "أنا أستمتع بالجرعة الأولى، ولا يحتاج الأمر بالنسبة لي سوى اتصال هاتفي بسيط، يصل العقار بعده إلى حيث أنا، إنه طقس بديع أشبه بفنجان قهوة الصباح"(٦٠).

ما هي مصادر المعلومات عن المخدرات على الإنترنت؟

تتنوع مصادر المعلومات على الإنترنت، فمنها فردي أو جماعي أو من خلال الجناة أو المروجين. تشمل مصادر المعلومات على الشبكة المصادر الآتية:

١- جناة المخدرات: وتستخدم هذه الفئة الإنترنت لزيارة زبائنهم، من خلال إغواء فئات الشباب وغيرهم في الانغماس في تعاطي المخدرات. وقد تتصرف هذه الفئة بشكل فردي أو جماعي، وقد لا يتوقف إغواء بتعاطي الفئة على تعاطي المخدرات وإنما ارتكاب جرائم أخرى ذات صلة بتعاطي المخدرات مثل سرقة بطاقات الإئتمان والاحتيال والجرائم المالية العامة.

٢- مروجي ثقافة المخدرات: وتهتم هذه الفئة بشكل خاص بتوسيع فئة مجتمع المتعاطين، وذلك لإضفاء شرعية على نشاطاتهم غير الشرعية، وزيادة الضغط على صانعي القانون لتغيير القوانين الخاصة بالمخدرات أو تعديلها بما يسمح بإنتاج المخدرات وتهريبها أو الحصول عليها. وقد لا تكون هذه الفئة من الجناة المستخدمين للمخدرات أو ممن لا يغوون فئات

أخرى في النشاط الجرمي الخاص بالمخدرات ولكنهم من يسعون لاستخدام المخدرات والسيطرة سوء استخدام الانترنت.

٣- دعاء توسيع حريات التعبير: تقوم هذه الفئة بنشر معلومات على الإنترنت لتوسيع حدود حرية التعبير الذاتي، وهذه المعلومات قد تدفع بعض الفئات وخاصة المراهقين بخرق القوانين الخاصة باستخدام المخدرات ويصبحوا خطرين على أنفسهم أو غيرهم من خلال سوء استخدم المخدرات.

٤- دعاء التجديد: وهذه الفئات سواء كانت أفراداً أو جماعات تطالب بتعديل القوانين والبنى الاجتماعية والاقتصادية وتنشر المعلومات عن المخدرات على الإنترنت لدعم حالاتهم من خلال تكوين سلوكيات ثقافية مضادة، فقد يغروا فئات بعدم إطاعة القوانين الخاصة بالمخدرات أو إساءة استعمال المخدرات.

٥- المجموعات الأخرى الخارجة على القانون: وتستخدم هذه الفئات الإنترنت لتشجيع الصغار بإرتكاب الجرائم التي لا علاقة لها بالمخدرات أو أن تجعلهم ضحايا جريمة.

٦- المعلومات المتحركة: إن طبيعة الإنترنت تساعد في جعل مكان الخطورة والتهديد في الطلب على المخدرات قضية معقدة. فالمعلومات المتوافرة على الإنترنت عن المخدرات قد تكون ساكنة في لحظة ما ومتحركة ومنتشرة في لحظة ما وبسرعة مذهلة. إن هذا التدفق للمعلومات جزء من طبيعة الإنترنت(٦١).

إنتاج المخدرات على الإنترنت:

يوفر الوصول للإنترنت كميات كبيرة من المعلومات تتعلق بإنتاج المخدرات بما في ذلك من عمليات ووصفات ومكونات ومقادير، وهذه المعلومات متوافرة لصغار السن والمراهقين والمتعاطين. وإن هذه المعلومات ليست بالضرورة أن تكون دقيقة وصحيحة، فالمعلومات الخاطئة قد تقود إلى إصابات خطيرة أو أمراض وحتى أحياناً تؤدي للوفاة. كما أن أدوات الإنتاج متوافرة عبر الإنترنت والمواد الكيماوية اللازمة لإنتاج المادة المخدرة متوافرة أيضاً وحتى أن هذه المواد والمعدات رخيصة الثمن ويمكن وضعها في المطبخ أو غرفة النوم أو في التسوية في المنازل.

استخدام المخدرات على الإنترنت:

تباع المخدرات سواء القانونية منها أو غير القانونية بشكل واسع على الإنترنت وغالباً ما تتم الصفقات للمخدرات غير الشرعية عبر لوحات النقاش وغرف الدردشة بلغة مشفرة وترسل المخدرات إلى العنوان المعني. كما أنه يمكن تقديم المعلومات اللازمة لإنتاجها في المنزل(٦٢).

هوامش الفصل الرابع

١- سرحان سليمان السرحان: محمود عبد المنعم المشهداني - أمن الحاسوب والمعلومات - عمان: دار وائل، ٢٠٠١. حسن ١١٤-١١٥.

٢- ستيفن أ. موسكوف، مارك ج. سيمكن. نظم المعلومات المحاسبية لاتخاذ القرارات: مفاهيم وتطبيقات؛ ترجمة كمال الدين سعيد؛ مراجعة أحمد حامد حجاج؛ تقديم سلطان المحمد السلطان - الرياض: دار المريخ، ٢٠٠٢. حسن ٥٠٢-٥٠٣.

٣- المرجع السابق نفسه. حسن ٥٠٣-٥٠٤.

٤- المرجع السابق نفسه. ص ٥٠٤-٥٠٥.

٥- الشبكة القانونية - فرع القانون. جرائم الكمبيوتر والإنترنت: المعنى والخصائص والصور واستراتيجية المواجهة القانونية. منشور على موقع arab@w net- lawsubject. تم زيارته بتاريخ ٢٠٠٤/١١/١٢.

٦- عبد الفتاح بيومي حجازي. الأحداث والإنترنت: دراسة متعمقة عن أثر الإنترنت في انحراف الأحداث - الإسكندرية: دار الفكر الجامعيي، ٢٠٠٢. ص ٣٦.

٧- سليمان مصطفى أبكر. جرائم الحاسب الآلي وطرق المواجهة. مجلة الأمن والحياة، ع ٢٤٣، السنة الحادية والعشرون (أكتوبر / نوفمبر(: الرياض: أكاديمية نايف للعلوم الأمنية، ٢٠٠٢. ض ٥٠-٥١.

٨- الشبكة القانونية - فرع القانون. مرجع سابق . ص ٢٧-٢٨.

٩- ريتشارد ماتسفيلد. حيل وأساليب الهاكرز وطرق الوقاية منها؛ الإعداد والترجمة خالد العامري (وآخروةن): القاهرة : دار الفاروق، ٢٠٠١. ص ٣٢-٣٣.

١٠- المرجع السابق نفسه. ص ٣٤-٣٥.

١١- الشبكة القانونية - فرع القانون، مرجع سابق. ص ٢٨-٣٠.

١٢- المرجع السابق نفسه. ص ٣١-٣٢.

١٣- ستيفن أ موسكوف ، مارك ج سيمكن، مرجع سابق. ص ٥٠٥-٥٠٦.

١٤- سليمان مصطفى أبكر. مرجع سابق. ص ٥١.

١٥- صالح بن محمد المسند، عبد الرحمن بن راشد المهيني. جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب م ١٥ ، ع ٢٩ .. الرياض: أكاديمية نايف العربية للعلوم الأمنية، ٢٠٠٠ ، ص ١٨٢-١٨٤.

١٦- المركز العالمي لدراسات وأبحاث الكتاب الأخضر : الإرهاب. - طرح - طرابلس: المركز، ١٩٩٠. ص ١١.

١٧- عادل نايف أبو ترابة: رؤية قانونية للإرهاب في المجتمع الدولي مجلة المؤتمر، ع ١٨. - طرابلس: المركز العالمي لدراسات وأبحاث الكتاب الأخضر، ٢٠٠٣. ص ١٧.

١٨- منير محمد الجنبيهي، ممدوح محمد الجنبيهي. جرائم الإنترنت والحاسب ووسائل مكافحتها. - الإسكندرية: دار الفكر الجامعي، ٢٠٠١، ص ٩٠-٩١.

١٩- نبيل علي. عنف المعلومات وإرهابها. في مستقبل الثورة الرقمية: العرب والتحدي القادم . - الكويت: مجلة العربي، ٢٠٠١، ص ١٥٠-١٥٢.

٢٠- شريف درويش اللبان تكنولوجيا الاتصال: المخاطر والتحديات والتأثيرات الاجتماعية - القاهرة: الدار المصرية اللبنانية، ٢٠٠٠ ص ١٣٥-١٣٦.نبيل علي. مرجع سابق ص ١٥٥-١٥٧.

٢١- هربرت أ. شيالر. المتلاعبون بالعقول؛ ترجمة عبد السلام رضوان. - الكويت: المجلس الوطني للثقافة والفنون والآداب. (سلسلة عالم المعرفة؛ ٢٤٣)، ١٩٩١ ص ٧-٨، ص ١٠-١٢.

٢٢- المرجع السابق نفسه ص ٢٠ ، ص ٣٨-٣٩.

٢٣- المرجع السابق نفسه ص ٤٢-٤٥.

٢٤- المرجع السابق نفسه ص ٤٢-٤٥.

٢٥- جعفر حسن جاسم - تكنولوجيا الإعلام العربي وهموم الواقع: دراسة نقدية في زحرحة الحدود (بحث تحت الطبع).

٢٦- بسيوني إبراهيم حمادة. العلاقة بين الإعلاميين والسياسيين في الوطن العربي. مجلة عالم الفكر، م ٢٣، ع١ و ٢ (يوليو/ سبتمبر - اكتوبر/ ديسمبر). - الكويت: المجلس الوطني للثقافة والفنون والآداب. ١٩٩١، ص ٢٠٨.

٢٧- شريف درويش اللبان. مرجع سابق. ص ١٣٣-١٣٤.

٢٨- عادل عبد الجواد محمد. إجرام الإنترنت: مجلة الأمن والحياة، ع ٢٢١ (ديسمبر/ يناير)، ٢٠٠١، ص ٧١.

٢٩- محمد: أمين الرومي. جرائم الكمبيوتر والانترنت. - الإسكندرية : دار المطبوعات الجامعية، ٢٠٠١، ص ٢٨-٢٩.سليمان مصطفى أبكر. مرجع سابق. ص ٥٠.

٣٠- محمد أمين الرومي. مرجع سابق. ص ٢٧-٢٨.

٣١- عادل عبد الجواد محمد. مرجع سابق. ص ٧١-٧٢.

٣٢- محمد أمين الرومي. مرجع سابق. ص ٥٦-٥٨.

٣٣- المرجع السابق نفسه. ص ٥٩-٦٠.

٣٤- شريف درويش اللبان. مرجع سابق. ص ١١٧-١١٩.

٣٥- نانسي سترن وروبرت سترن. الحاسبات في هصر المعلومات؛ ترجمة سرور علي إبراهيم سرور وهندي عبد اللـه العلي الهندي. الرياض: دار المريخ، ١٩٨٨. ص ٨٤٥-٨٤٦.

٣٦- بيهسن فرعون. الشبكات العصبية آفاق جديدة للذكاء الاصطناعي. مجلة العربي، ع ٥ ديسمبر (كانون أول). - الكويت: وزارة الإعلام، ١٩٩٥، ص ٨٨.

٣٧- عادل عبد الجواد محمد - مرجع سابق. ٧٢.

٣٨- عبد الفتاح بيومي حجازي. مرجع سابق ص ٢٦٠-٢٦٥.

٣٩- عادل عبد الجواد. مرجع سابق ص ٧٢.

٤٠- شريف درويش اللبان: رؤية مستقبلية للجوانب الأخلاقية للمعلومات في الوطن العربي. مجلة البحوث والدراسات العربية، ع ٣٣. - القاهرة: معهد البحوث والدراسات العربية، ٢٠٠٢. ص ١٨١.

٤١- محمد أمين الرومي. مرجع سابق ص ١٣٣-١٣٦.

٤٢- أيمن السيد عدلي. الاختراق والتجسس في عالم تكنولوجيا المعلومات. مجلة التقدم العلمي، ع٤٦ - الكويت: مؤسسة التقدم العلمي، ٢٠٠٤. ص ٧٧.

٤٣- لمزيد من المعلومات أنظر الأساطير الإفريقية.

٤٤- محمد أمين الرومي. مرجع سابق. ص ١٣٦-١٣٧.

٤٥- أيمن السيد عدلي. مرجع سابق. ص ٧٩.

٤٦- المرجع السابق نفسه ص ٧٩-٨٠.

٤٧- شريف درويش اللبان. تكنولوجيا الاتصال: المخاطر والتاثيرات الاجتماعية. مرجع سابق. ص ١٣١-١٣٢.

٤٨- المرجع السابق نفسه. ص ١٣١.

٤٩- لمزيد من المعلومات عن مثل هذه الحالات راجع كتاب الأحداث والإنترنت لعبد الفتاح بيومب حجازي.

٥٠- محمد أمين الرومي. مرجع سابق. ص ١٣٠.

٥١- شريف درويش اللبان أخلاقيات المعلومات في العصر الإلكتروني: رؤية مستقبلية للجوانب الأخلاقية للمعلومات في الوطن العربي. مرجع سابق . ض ١٨١.

٥٢- عبد الفتاح بيومي حجازي. مرجع سابق. ص ١٢٨.

٥٣- هدى حامد قشقوش. جريمة غسيل الأموال في نطاق التعاون الدولي. - القاهرة، دار النهضة العربية، ٢٠٠١. ص ٦٢-٦٣.

٥٤- هدى حامد قشقوش. مرجع سابق. ص ٧ ، ص ٥-٦.

٥٥- المرجع السابق نفسه ص ١٩.

٥٦- عبد الفتاح بيومي حجازي. مرجع سابق ص ٧٧-٧٩، ص ٨٤-٨٥، ص ٨٩-٩٠.ذياب البداينة. التحديات الأمنية في عصر العولمة . مجلة الدراسات الأمنية، ع١، عمان : مديرية الأمن العام، ٢٠٠٤. ص ١٩.

٥٧- عبد الفتاح بيومي حجازي. مرجع سابق ص ١٠٤-١٠٥.

٥٨- المرجع السابق نفسه. ص ١٠٧ ، ص ١١٢-١١٣.

٥٩- ذياب البداينة، مرجع سابق . ص ١٦-١٧.

٦٠- المرجع السابق نفسه. ص ١٧-١٨.

الفصل الخامس




مكافحة جرائم
تكنولوجيا المعلومات

تقديم

إن ارتباط الأفراد، بل المنظمات والدول مع بعضها البعض، عن طريق شبكة المعلومات العالمية (الإنترنت)، وازدياد عدد المستخدمين والمستفيدين من خدمات الإنترنت والتي أصبحت خدماتها عابرة للحدود، فرض على الأفراد والدول على حد سواء ضرورة التفكير بإيجاد طرق وأساليب جديدة لمكافحة جرائم تكنولوجيا المعلومات، على الصعيد الفردي والدولي.

بيد أن أمر مكافحة جرائم تكنولوجيا المعلومات لا يخلو من صعوبات ومشكلات، وعليه لا بد من الاعتراف بأنه بات مؤكدا أن يعرف المجتمع بأنه لا يوجد حل جذري يُنصح الالتزام به لتجنب شر أو الوقاية من جرائم تكنولوجيا المعلومات. وتأتي صعوبة الموقف هنا، نتيجة لتنوع أشكال هذا النوع من الجرائم، أضف عليه، تعدد طرق وأساليب ارتكابها، زد على ذلك اختلاف دوافع وصفات مرتكبيها.. الخ.

يتضح مما سبق، إن مكافحة جرائم تكنولوجيا المعلومات على المستوى الشخصي، بل وعلى صعيد مستوى الدولة الواحدة، لن يكون مجدياً أو لن يكون له أي تأثير يذكر، إلا إذا كان هناك تعاوناً دولياً على أكبر قدر من التنسيق والتعاون بين الأفراد والمنظمات والشركات والدول، وأمام هذه الجهات جميعاً، بات لزاماً وضع استراتيجيات أمنية شاملة لنظم المعلومات يجب أن يكون منطلقة من التعاون الدولي على كافة المستويات، ومن ثم العمل على تنسيق تلك الجهود المبذولة بين كافة دول العالم لتكون هناك أسس ومبادئ وقوانين وثقافة يمكن الاعتماد عليها لخلق مواطن لديه وعي عالمي يجنبه عملياً عدم الانزلاق وراء دوافعه لارتكاب إحدى جرائم تكنولوجيا المعلومات أولاً، قبل الخوف من الردع القانوني ثانياً.

١- المشكلات التي تقف وراء صعوبة المكافحة.

قد عرفت المجتمعات الإنسانية ومن خلال تاريخها الطويل عدداً لا يحصى من اشكال وأنواع الجرائم التقليدية منها، والحديثة أو المتجددة وفقاً لتجدد معطيات العصر الحاضر، أضعف على ذلك، أن الإنسان حاول أن يحدث تغييراً جذرياً في مساره التاريخي وصراعه مع الطبيعة من خلال إستيعابه لعناصر التغيير الفعال، لاسيما تلك التي تؤسس طريق المستقبل وبشكل أخص العناصر المستحدثة، وإلا فإن العنصر قد ينقلب على أزمة حقيقية إن لم يفهم ويتعامل معه بشكل جيد، ومن هذه التحديات التاريخية التي باتت ظاهرة تواجه مجتمع المعلومات الحديث هي صعوبة

مكافحة جرائم تكنولوجيا المعلومات، هـذه الظـاهرة التـي فرضـت نفـسها فرضـاً عـلى أمـم وشـعوب المجتمعـات المتطورة منها، وغير المتطورة على حدٍ سواء.

وفقاً لما تقدمن يمكن القول: عن المعرفة الإنسانية تشكل العنـصر الأسـاسي في صـنع الحركـة التقدميـة للأمـم وبنـاء التاريخ الإيجابي، لأن الإنسان بتميزه التكويني يعتمد أساساً على التشكل المعرفي لبناء شخصيته واكتساب ثقافتـه ونمـوه العلمي لإشباع حاجاته المادية والمعنوية، حيث يمثل إنتاجه الفكري واسـتنتاجاته العقليـة وسـيلة سـلوكية للتعامـل مـع الواقع الخارجي وفهم المحيط الذي يعيشه لاكتساب المزيد من الخبرات والتجـارب وإيجـاد حالـة التـأقلم مـع الظـروف الخارجية لصنع حياة أفضل بالنسبة له.(١)

أمام تلك المعطيات والتي كانت تشكل تحدياً كبيراً للإنسان، كان لزامـاً عـلى الإنـسان ومنـذ بـدء الخليقـة مواجهـة مشاكله أو الحصول على احتياجاته من خلال زيادة قدراته الذاتية والاستفادة من بناء أدوات ومعدات، مـما تـسمح لـه به الطبيعة من نباتها وصخورها وخاماتها ومعادنها والسيطرة على حيواناتها، أو باستخدام آلات مـما أنـتج الإنـسان مـن خاماتها، وفي النهاية فهي جميعاً تتمثل في رفع وزيادة لقدراته العملية ضماناً لأمنه وأمـن الإنـسانية، وتحـسيناً لأسـلوب حياته وقد تغيرت نوعيات الآلات والمعدات والقوى المحركة عبر العصور مما نقله من نوعية مجتمع إلى آخـر. ذلـك أنـه قد أعقب كل تطور في إمكانيات الإنسان العملية تغير في أسلوب حياته، استلزم منه عمل إضافات، مما أدى إلى اضـطراد التطوير (٢).

وتواجه اليوم كل من الدول المتقدمة والدول النامية على حدٍ سـواء خطـر هـذا التطـور، لاسـيما التكنولـوجي منـه، حيث إن جرائم تكنولوجيا المعلومات باتت تهدد المجتمعات الإنسانية وتنبأهـا بمخـاطر وخـسائر اقتـصادية واجتماعيـة وسياسية هزّت مضاجع الكبار والصغار من ساسة ورجال اقتصاد وكذلك الحال ينطبق عـلى المؤسـسات الحكوميـة منهـا والأهلية.

يعترف العديد من المهتمين بـشؤون تكنولوجيـا المعلومـات، لا سـيما الجانـب المتعلـق بإرتكـاب الجـرائم، يعترفـون بصعوبة اكتشاف جرائم تكنولوجيا المعلومات، وكذلك في ذات الوقت يعترفـون بـصعوبة بالغـة جـداً في محاولـة منعهـا. وعملية الاعتراف هذه نابعة من وجود العديد من المشكلات والصعوبات العمليـة والإجرائيـة التـي تظهـر عنـد ارتكـاب أحد ما جريمة ما من جرائم تكنولوجيا المعلومات. ومن هذه المشكلات:

١. يمكن أن تنقضي عدة أشهر أو حتى سنوات قبل اكتشاف الجريمة.

٢. القوانين التي تحكم جرائم الحاسوب ليست واضحة ولم يسبق اختبارها مثل أنواع القوانين الأخرى.

٣. عادة ما تتردد المنظمات مثل البنوك، وشركات بطاقات الائتمان، وبيوت الاستثمارات في الإعلان عن الجريمة(٣).

٤. صعوبة إثبات وقوع الجريمة، في العديد من الحالات يتم الفعل الإجرامي دون أن يعلم المجني عليه بحدوث اعتداء وقع عليه، ومن ذلك أن يتم إدخال فايروس إلى الجهاز عن طريق الاتصال بشبكة الإنترنت، ويظل الفيروس كامناً حتى لحظة معينة، ثم يقوم النشاط وتدمير البرامج والمعلومات. فهنا المجني عليه لا يدري بالوقت الذي تم فيه إصابته بالفايروس، كما أن الفايروس ممكن أن يدمر نفسه في النهاية بحيث لا يعرف نوعية الفايروس أو من قام بإدخاله.

٥. صعوبة التوصل إلى الجاني: كثيراً ما يقوم الجاني بالدخول إلى شبكة الإنترنت باستخدام اسم مستعار وغالباً ما يقوم بالدخول على الانترنت عن طريق مقاهي الإنترنت وبالتالي يصعب معرفة الجاني وتحديد موقع اتصاله.

٦. صعوبة إلحاق العقوبة بالجاني المقيم: هناك صعوبة في حالة ما إذا تم ارتكاب الجريمة بواسطة شخص أجنبي مقيم في الخارج ووقت الجريمة في مصر . فهنا لا بد من تدخل الأنتربول الدولي للقبض على الجاني وإخضاعه للعقاب.

٧. تنازع القوانين الجنائية من حيث المكان: هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي وعينية القانون الجنائي، وشخصية القانون الجنائي، وعالمية القانون الجنائي. وتثور المشكلة في حالة ارتكاب الفعل المؤثم في الخارج، فأي من القوانين الجنائية سوف يخضع لها الجاني؟

٨. صعوبة تحديد المسؤول جنائياً عن الفعل الإجرامي: يظهر ذلك في حالة وقوع جريمة على شبكة الإنترنت، كأن يدخل المستخدم للشبكة على موقع فيجد به أفعال إباحية، فهل يسأل عن هذه الجريمة عامل الاتصال أم مورد المنافذ أم مورد المعلومات أو غير ذلك من العاملين في مجال الإنترنت.

٩. القصور في القوانين الجنائية القائمة: أدى ذلك القصور ومحاولة الفقه والقضاء إلى إخضاع جرائم الإنترنت إلى نصوص قانون العقوبات، إن توسع الفقه والقضاء في تفسير النصوص الجنائية القائمة خاصة بالنسبة للوضع في فرنسا وأمريكا، فجرائم الإنترنت هناك تعتبر من جرائم الصحافة باعتبار أن شبكة الانترنت من وسائل النشر، فهي تعد وسيلة نشر إلكترونية.

١٠. افتراض العلم بقانون جميع دول العالم: فالشخص الذي ينوي ارتكاب جريمة من جرائم الإنترنت فيقوم بالنشاط الإجرامي في دولته، وتتحقق النتيجة في دولة أخرى يخضع للقانون الجنائي لتلك الدولة التي تحقق فيها النتيجة الإجرامية، وهنا يجد الشخص نفسه خاضعاً لقانون دولة لا يعرف عنه أي شيء على أساس أن جميع دول العالم تفترض العلم بقانونها، حيث يسود مبدأ عدم جواز الاعتذار بالجهل بالقانون. فيمكن تصور الفعل الذي اتاه الشخص في دولته فعل مباح ولكنه يشكل جريمة في الدولة التي تحقق فيها نتيجة فعله. ويعد ذلك الأمر غير مقبول.

١١. صعوبة السيطرة على أدلة ثبوت الجريمة: حينما يتحدد مكان ارتكاب الجريمة التي تمت بواسطة استخدام شبكة الإنترنت ويتوجه أفراد الضبطية القضائية للقبض على الجاني وتحرير أدلة الجريمة ومنها جهاز الكمبيوتر المستخدم في الاتصال بالشبكة وما يحويه من برامج ومعلومات. تثور مشكلة معرفة الرقم السري الذي بدونه لا يعمل جهاز الكمبيوتر، وفي هذه الحالة لا يجوز لأجهزة التفتيش إجبار المتهم على الإفشاء عن الرقم السري، حيث يعد ذلك إجراء غير قانوني، كذلك قد يتمكن الجاني من تدمير البيانات المخزنة داخل الكمبيوتر والتي تعد دليل إدانته في ثوان معدودة اثناء إجراء التفتيش، كذلك قد يحتوي جهاز الكمبيوتر على ملفات سرية لا يجوز للغير الاطلاع عليها، حيث يعد الاطلاع عليها مشكلة لجريمة انتهاك حرمة الغير، ففي هذه الحالات المختلفة يكون هناك صعوبة في جمع الأدلة المادية التي تثبت ارتكاب إحدى جرائم الإنترنت.

١٢. صعوبة المطالبة بالتعويض المدني: هناك صعوبة بالنسبة للمطالبة بالتعويض المدني عن ارتكاب أحد جرائم الإنترنت، حيث يرجع في ذلك لأحكام القانون الدولي الخاص وما يثيره من صعوبات واتجاهات فقهية وتشريعية معارضة.(٤).

١٣. جهل الناس بثقافة الإنترنت: حيث إن الأغلبية مـن البـشرية لا يعـرف الكثـير عـن الإنترنـت، وحتـى أولئـك الـذين يستخدمونها، مما يقعون في أحيان عديدة في مطبات أو أخطاء لا يفطنون بها، إلا أنها مـن الناحيـة القانونيـة تعـد جريمة ويحاسب عليها القانون.

١٤. جهل المؤسسات أو مقاهي الإنترنت كذلك بجرائم تكنولوجيا المعلومات: هناك العديد من النـاس الـذين يعيـشون أو يكتسون لقمة عيشهم مـن وراء عملهـم في منتـديات أو مقـاهي الإنترنـت، وكـذلك المـسؤولين عـن إدارة هـذه المنتديات والمقاهي، هؤلاء جميعاً لا يعرفون شيئاً عن جـرائم تكنولوجيـا المعلومـات، ولـو كـانوا يعرفـون لوضـعوا لافتتات تحذير للزبائن لماهية جرائم تكنولوجيا المعلومات، وكذلك وجود إشارة للعقوبـات القانونيـة التـي تترتـب على واحدة من هذه الجرائم ولو بشكل مختصر.

لكن ورغم هذه المشكلات والصعوبات التي واجهت وتواجه المجتمع، لاسيما المعنيـون بمكافحـة جـرائم تكنولوجيـا المعلومات، لم تهبط إرادة أصحاب عقول المعرفة والتقنية التكنولوجية، ورجال القانون والأمن، في إيجاد أو ابتكار قـوانين وطرق وتكنولوجيا معلومات قادرة على استكشاف المجرمين وإمكانية ملاحقتهم لإنـزال العقوبـة القانونيـة التـي تتـوائم وفعلهم الإجرامي.

٢- طرق وأساليب مكافحة جرائم تكنولوجيا المعلومات:

لقد حدثت تغيرات كبيرة، بل ونوعية في عـالم اليـوم، وسـوف تـستمر تياراتهـا وتوجهاتهـا وتأثيرهـا إلى فـترة طويلـة وعميقة في هذا القرن، ومما لا شك فيه أن تلك التغيرات سـوف تـشكل انعطافـاً حـضارياً في مـسيرة التنميـة وأبعادهـا الاجتماعية. يمكن القول: إن من خلال استعراض أنواع جرائم تكنولوجيا المعلومات، إن الـدافع وراء أغلـب تلـك الجـرائم هو دافع مادي، ويرى "تومـاس فريـدمان" أن الأمـل الوحيـد أمـام الفقـراء هـو أن يتـذكرهم الأغنيـاء، ذلـك لأن الـدول المتقدمة والمتحكمة تكنولوجيا تتحكم في نصف رأس المال العالمي، فضلاً عن تحكمها في الأسواق الماليـة والمـضاربة فيهـا. يصل هذا التحكم إلى وجود مؤسسات عقابيـة أمثـال " سـتاندرودوبورز" (standard and poors) ، و" مـودي" (moody)، ويوكل إليها مهمة المراقبة على الـدول والمؤسـسات لمراقبـة مـدى التزامهـا بـشروط العولمـة وقوانينهـا.(٥) وأمـام عولمـة الجريمة عبر تكنولوجيا المعلومات بات لزاماً على المجتمعات الإنسانية، أن تفتش عن طـرق وأسـاليب جديـدة مـن أجـل التصدي لهذا النوع من الجرائم. وفيما يلي أهـم الطرق والأساليب التي يمكن أن تنجح في مجال المكافحة:

أولاً: التربية والأخلاق قبل كل شيء:

إن الإنسان هو غاية التربية ، كما هو غاية التنمية للبناء والتطور، ووسيلتها سواء كانت تتعلق ببناء الإنسان ذاته أو بناء المجتمع الذي يعيش فيه. ويعرف الدكتور (جون هانسون) التنمية بأنها عملية الارتقاء بمستوى الإنسان ارتقاءً تتضافر فيه جهود الأمة أفراداً وجماعات، منظمات ومؤسسات على كافة المستويات من أجل تحسين مستوى الحياة ورفع مستوى الأمة من حالة الركود والتخلف إلى حالة النمو والتقدم.(٦).

إن مفهوم التربية والنظرة إليها يختلف من مجتمع إلى آخر، ومن أمة إلى أخرى، ومن عصر على آخر، فالتغير هو صورة الحياة، والأختلاف هو طبيعية البشر وناموس الكون ومن النادر أن نجد أمة من الأمم أو شعباً من الشعوب يتفق كلية مع غيره في فكره وتفكيره ورؤاه حول قضايا وأموره المصيرية.

لقد كان مبدأ الفضيلة وتنمية الأخلاق الحميدة والسلوك المتزن والمواظبة الصالحة من أهم أهداف التربية اليونانية، كما يظهر ذلك في فكر (أفلاطون) و (أرسطو)، كذلك في الفكر الغربي نجد أن (سانت توماس أكويناس) يؤكد بأن الهدف من الحياة والتربية هو تحقيق السعادة عن طريق غرس الفضائل العقلية باعتبار أن الأخلاق أساس التعامل وعنوان الأمم ورمز تطورها وبقائها، كما قال الشاعر:

وإنما الأمم الأخلاق ما بقيت   فإن همو ذهبت أخلاقهم ذهبوا

يهدف الغرض الاجتماعي في التربية إلى إعداد الفرد ليعيش في مجتمعه ويتعامل مع أفراده تعاملاً صحيحاً يعود عليه وعلى مجتمعه بالخير والفائدة، وأن يكون قادراً على معايشة من حوله ومبادلتهم الإستعداد للتعاون والتضحية والتكافل الاجتماعي (٧). ومن هنا يمكن القول : إن مكافحة كل الجرائم ولا سيما جرائم تكنولوجيا المعلومات تعتمد أولاً وقبل كل شيء على مبدأ التربية وإعداد الفرد إعداداً اجتماعياً سليماً، ولذلك فإن موضوع التربية يعد من أخطر وأهم المواضيع التي واجهت ولا زالت تواجه المجتمعات الإنسانية، وذلك لما لها من دور مؤثر، بل وفعال في بناء الحضارة الإنسانية.

يرى (جيفرسون) أن التربية ضرورية لبناء الإنسان العصري المتمكن بسلاح العلم وبعمق التجربة التي يستطيع بواسطتها معرفة ذاته ووجوده والقدرة على اتخاذ القرار الصائب في كل

أمور حياته، بيد أن (هوراس مان) العالم الأمريكي الشهير الذي عرف بلقب "أب التعليم"، نظر إلى القضية نظرة أعمق من ذلك فقد رأى أنها قضية أساسها الإرتقاء الأخلاقي، فكتب يقول: (لن تستقر الحكمة في دول التشريع، ولن يدون كلامها في سجل القانون حتى تخلق المدارس العامة ذكاءً أبعد أفقاً ، وخلقاً أنقى لدى كل طلاب العلم وراغبي المعرفة مما ظهر حتى الآن في الولايات المتحدة الأمريكية.(٨)

وفقاً لما تقدم يمكن القول: إن هناك العديد من الجرائم التي ترتكب يومياً، وكثيرا ما نضع اللوم على هذه الآلة أو تلك التي تسببت في إيذاء أو قتل هذا الإنسان أو ذاك، ناسين أو بالأحرى متناسين أن السبب ليس هذه الآلة التكنولوجية أو تلك وراء ذلك الفعل الإجرامي، وإنما الإنسان هو الذي يقف أولاً وأخيراً إزاء كل ما يرتكب من أفعال إجرامية بحق أخيه الإنسان في الحياة. وعادة ما تحدد تلك الأفعال الإجرامية أو الخيرة بالمبادئ والأخلاق والقيم التي تربى عليها الإنسان، فهي المعيار الأول الذي بموجبه يرتكب أو لا يرتكب الإنسان فعل إجرامي.

إن التكنولوجيا بطبيعتها (متعادلة القيمة Valueneutal)، فالسيف كأي تكنولوجيا لا يختلف عن الصخور ، والهواء، أو الماء، أي أنه خامة تكنولوجيا، إنه ببساطة مجرد خامة جامدة، والأشياء بذاتها لا تحمل قدراً من الخير أو الشر، وإنما البشر هم الذين ينفثون فيها الحياة باستخدامهم إياها ويضفون عليها خصائص معنوية وأخلاقية.

قد يبقى السؤال الأهم والذي كثيراً ما يردده الناس مفاده: هل هناك تكنولوجيا تحمل طبيعة طيبة أو شريرة متأصلة؟ وربما تكون الإجابة حاضرة في أذهان الناس، بيد أن هذه الإجابة تبقى تمثل وجهة نظر كل واحد منا. فعلى مر العصور كان البعض ينظر إلى تكنولوجية ما على أنها مفيدة، بينما يراها البعض الآخر مصدراً للضرر والأذى، هكذا هم الناس في كل زمان ومكان، إنها الطبيعة الإنسانية تحمل بين ثناياها الخير والشر ولكل واحد منها مقدار (إن كل شيء خلقناه بقدر) (٩).

حتى اليوم لا ينبغي الخلط بين التكنولوجيا والأخلاق . ولنأخذ الطاقة النووية على سبيل المثال فإننا نزود مدننا بتلك الطاقة، كما نصنع القنابل ونشيد الغواصات النووية. وعندما يتم الترويج للقنابل والغواصات على أنها أسلحة للدفاع ليست للهجوم، فإن الخط الفاصل بين الخير والشر يصبح ضبابياً غير واضح المعالم، ولنضرب مثالاً آخر لآلة حادة، إنها (السكين)، فمن الممكن استخدامها في تقطيع اللحم والفاكهة في المطبخ أو في ارتكاب جريمة قتل، وهكذا نجد أن أي

تكنولوجيا ما هي إلا أداة ، والأدوات يمكن استخدامها لأغراض متعددة، فهي مجرد عدسة لامة تركز الاهتمام على جميع القضايا الأخلاقية والمعنوية التي يتحتم على المجتمع أن يتوافق معها.

منذ ظهور جماعة محطمي الماكينات (luddit) في إنجلترا في بداية القرن التاسع عشر، ترسب عند الناس كراهية لأي تقدم تكنولوجي، فقد قام هؤلاء الرجعيون بالثورة ضد ماكينات النسيج المستحدثة التي كانت تهدد مصدر رزقهم كنساجين، فما كان منهم إلا أن قاموا باقتحام المصانع وتدمير الأموال الميكانيكية الجديدة، فقد كانوا يخشون أن تؤدي التكنولوجيا الجديدة إلى قطع مصدر عيشهم وتدمير نمط حياتهم الذي اعتادوه، وينطبق ذلك تماماً في القرن العشرين على خطوط تجميع السيارات.

مع كل مرحلة من التطور التكنولوجي ، كان يثور جدل من نوع ما، وطالما كان التلفاز أداة جذب لذلك النوع من الجدل. فهل من المعقول عندما تستشري الأوبئة الاجتماعية، هل نوجه اللوم إلى التلفاز أم إلى المجتمع الذي يسمح بتصوير العنف من خلاله؟ وهل نحن على استعداد للتضحية بالقيم الأخلاقية الأساسية لدينا وبأمن وسلامة مجتمعنا على مذبح الحرية الشخصية؟ وهل للأفراد الحق في تصوير أفعال خادشة للحياء والأخلاق دون اعتبار لتأثيرها الواسع النطاق في المجتمع؟ إن كل هذه القضايا والتساؤلات يثيرها التلفاز والصيغ الأخرى للتكنولوجيا الإعلامية، وهي على أي حال ليست وليدة التكنولوجيا.(١٠)

كلما إزدادت الأداة تعقيداً، ازداد تحديها للمجتمع كي يتحكم فيها على نحو مسؤول . وإذا كنا لا نقبل العنف في الطرقات، فلماذا نقبل مشاهدته في التلفاز أو ممارسته في أحد ألعاب الفيديو؟ فهذه ظواهر إنسانية تستدعي العديد من المسؤولين والمهتمين بالشرون النفسية والاجتماعية ومن ثم أهل القانون الوقوف عندها، لكي يخرج الجميع بنتائج تغير جميع فئات المجتمع.

ثمة موضوع واحد لا يرقى إلى الشك. وهو أن إلقاء التبعة على التكنولوجيا ليس هو الحل. فلننظر إلى ذواتنا ومجتمعنا، ونتأمل معايرنا وقيمنا. وفي الوقت ذاته علينا أن نأخذ حذرنا في مواجهة أولئك الذي ينادون بوقف التقدم التكنولوجي باسم المحافظة على الأخلاق إن تركيزنا يجب أن ينصب على كيفية استخدام الأدوات والوسائل التكنولوجية، ويجب ألا ينصب على كيفية استخدام الأدوات والوسائل التكنولوجية، ويجب ألا ينصب تفكيرنا على الأدوات والوسائل، بل على كيفية استخدامها.(١١) ويجب أن يكون استخدامها وفقاً لمبادئ وقيم وأخلاق حميدة وفاضلة يجب أن تزرع في نفوس الصغار قبل الكبار، فالتربية والتعلم منذ الصغر

كالنقش على الحجر، ومن هنا تنطلق عملية مكافحة كل العادات والتقاليد والأفعال التي لا تتلائم مع المبادئ والأخلاق والقيم الصحيحة وكل منظومة القيم الاجتماعية الفاضلة التي زرعت في نفوس الأجيال سواء في البيت أو المدرسة، وتعد المبادئ والقيم والأخلاق ومنظومة التربية الحسنة أهم سلاح يمكن أن نجابه به ونتصوى لكل الجرائم ومنها جرائم تكنولوجيا المعلومات.

ثانياً: المعاهدات والمؤتمرات الدولية:

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، ومن تلك المعاهدات:

١- معاهدة بودا بست لمكافحة جرائم الإنترنت:

The BUDAPEST CONVENION ON CYPER CRIMES

شهدت العاصمة المجرية بودا بست في أواخر عام (٢٠٠١) ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت "INTERNET CRIMES" وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها لاسيما بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات.

يعد التوقيع على تلك المعاهدة الدولية هو الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم على شبكة الإنترنت واستخدامها الاستخدام الأسوأ، حيث تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت، والتي انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الأغلب الأعم من الحالات ودون أي غرض إجرامي إلى مرحلة جديدة يقوم بها محترفون على "أعلى درجة من التخصص، وتتمثل في الاحتيال والاختلاس وجرائم تهديد الحياة وهي قضايا تعرض حياة وممتلكات العديدين من رواد شبكة الإنترنت للخطر.

إن التوقيع على تلك الاتفاقية من قبل المسؤولين في الدول الأوروبية.

إضافة إلى أمريكا واليابان وكندا وجنوب أفريقيا هو نتاج مباحثات ومفاوضات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الاتفاقية ومن ثم التوقيع عليها من جميع الأطراف .

لقد جاءت معاهدة بودابست لمكافحة جرائم الإنترنت بعد إجراء العديد من الدراسات على مجال التضامن الدولي في مكافحة جرائم الإنترنت أوضعت أن العديد من الدول لا تستطيع بمفردها مواجهة تلك الجرائم التي ترتكب عبر الإنترنت مهما سنت من قوانين ومهما غلظت من عقوبات تلك الجرائم؛ نظراً لكون تلك الجرائم هي من الجرائم عابرة الحدود التي لا يقف أمامها أي عائق جغرافي ، وبالتالي فتلك الدول تفضل الانضمام إلى المعاهدات الدولية التي تبرم في هذا المجال نظراً لكبر حجم الأضرار عن طريق الإنترنت؛ ولأن العديد من الدول حتى المتقدمة منها لا تستطيع مواجهة تلك الأخطار بمفردها دون وجود تعاون وتضامن دولي ليتم نجاح أي مجهودات تبذل في مجال مكافحة الجرائم التي ترتكب عبر الإنترنت، أن التعاون الدولي في تطبيق تلك القوانين هو الطريق الوحيد ليتم احترام حقوق الإنسان مثل الحقوق الملكية الفكرية للإنسان.

من ضمن الجوانب العديدة التي تناولتها تلك الاتفاقية الإرهاب الإلكتروني وعمليات تزوير بطاقات الإئتمان ودعارة الأطفال، وتلك الجرائم تعتبر من أكثر الجرائم انتشاراً على المستوى العالمي بصفة عامة وفي أوربا بصفة عامة وفي أوربا وأمريكا بصفة خاصة ولم تفلح أي جهود فردية تم بذلها من جانب أي من الدول الموقعة على الاتفاقية، وعليه فقد كان من المحتم التنسيق بين تلك الجهود على أقل تقدير أن لم يكن التوحيد بينها لتؤتي ثمارها في الحد من ارتكاب تلك الجرائم التي تؤثر على التقدم الاقتصادي المتواصل في اقتصاديات تلك الدول المتقدمة. كذلك تحدد الاتفاقية أفضل الطرق الواجب إتباعها في التحقيق في جرائم الإنترنت التي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها.

٢- المعاهدة الأوروبية لمكافحة جرائم الإنترنت:

وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة جرائم الإنترنت وسط انتقادات من دعاة حماية الحرية الشخصية، وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدان المعنية ستلزم الاتفاقية الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالمية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبيانات وجرائم الاحتيال والتزوير التي لها صلة بالكمبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي.

تتضمن بنود المعاهدة التي تم تعديل مسودتها (٢٧) مرة قبل الموافقة عليها، فقرات تكفل للحكومات حق المراقبة وتلزم الدول بمساعدة بعضها في جمع الأدلة وفرض القانون، لكن الصلاحيات الدولية الجديدة ستكون على حساب حماية المواطنين من إساءة الحكومات استخدام السلطات التي أعطتها لهم تلك الاتفاقية التي قد يسيئون استخدامها.(١٢)

ثالثاً: إصدار قوانين جديدة تجرم الجرائم الإلكترونية في كافة أنحاء العالم بحيث يكون بينها قدراً كبيراً من التناسق:

اتجهت كافة الدولة المتقدمة تكنولوجيا إلى استحداث نصوص قانونية جديدة تجرم الجرائم الإلكترونية الجديدة على قوانينها التقليدية القديمة، وعليه فقد صاغت تلك الدول نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة تكنولوجياً.

أ- على المستوى العالمي:

تعد دولة السويد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الإنترنت والحاسب الآلي لتستطيع أن تعاقب المتهمين بارتكاب تلك الجرائم الإلكترونية، حيث صدر أول قانون خاص بها (The Special low) وسمي بقانون (البيانات)، وقد صدر هذا القانون عام (١٩٧٣)ن وقد عالج هذا القانون قضايا الاحتيال عن طريق الإنترنت بالإضافة إلى كونه يشتمل على فقرات عامة من نصوصه لتشمل جرائم الدخول غير المشروع على البيانات الإلكترونية أو تزوير المعلومات الإلكترونية أو تحويلها أو الحصول غير المشروع عليها.

أما الولايات المتحدة الأمركية فكانت هي الدولة التالية التي تبعت السويد في إصدار قوانين خاصة بها (Special laws)، تجرم الجرائم الإلكترونية ، حيث شرعت قانوناً خاصً بحماية أنظمة الحاسب الآلي (١٩٨٥-١٩٧٦) وفي عام (١٩٨٥) حدد معهد العدالة القومي الأمريكي خمسة أنواع رئيسة للجرائم المعلوماتية ، وهي:

١- جرائم الحاسب الآلي الداخلية.

٢- جرائم الحاسب غير المشروع عن بعد.

٣- جرائم التلاعب بالحاسب الآلي.

٤- دعم التعاملات الإجرامية.

٥- سرقة البرامج الجاهزة والمكونات المادية للحاسب.

وفي عام (١٩٨٦) صدر قانوناً يحمل رقم (١٢١٣) عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت المتطلبات الضرورية اللازمة لتطبيقه. وعلى أثر ذلك قامت الولايات الداخلية بإصدار التشريعات الخاصة بكل منها على حده للتعامل بها مع تلك الجرائم الإلكترونية ومن تلك القوانين ، القانون الخاص بولاية تكساس لجرائم الحاسب الآلي. وقد خولت وزارة العدل الأمريكية في عام (٢٠٠٠) خمس جهات حكومية للتعامل مع جرائم الإنترنت والحاسب الآلي منها مكتب التحقيقات الفيدرالي (FBI).

أما بريطانيا فهي ثالث دولة تسن قانوناً خاصاً بها (Special law) بجرائم الإنترنت، حيث أقرت قانوناً لمكافحة التزوير والتزييف عام (١٩٨١) الذي تشمل في تعاريفه الخاصة تعريف أداة التزوير، وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق الإلكترونية أو التقليدية أو أي طرق أخرى.

أما كندا فهي تطبق قوانين متخصصة ومفصلة للتعامل مع جرائم الإنترنت، حيث عدلت في عام (١٩٨٥)، قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت كما شمل القانون الجديد أيضاً تحديد للعقوبات المطبقة على المخالفات الحاسوبية وجرائم التدمير وجرائم الدخول غير المشروع على المعلومات الإلكترونية، كما وضح القانون صلاحيات جهات التحقيق، كما جاء في قانون المنافسة الذي يخول لمأمور القبض القضائي متى حصل على أمر قضائي حق التفتيش على أنظمة الحاسب الآلي والتعامل معها وضبطها.

أما الدنمارك فقد انتهت لهذا الأمر مبكراً أيضاً فقد سنت أول قانون خاص بها في مجال مكافحة جرائم الإنترنت والحاسب الآلي في عام (١٩٨٥) ، وقد شمل القانون العقوبات المحددة على ما يرتكب من جرائم مثل الدخول غير المشروع إلى الحاسب الآلي أو تزوير البيانات سواء كان هذا التزوير بالحذف أو بالإضافة أو بالتعديل.

أما فرنسا فهي من الدول التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع الجرائم التكنولوجية الحديثة (جرائم الإنترنت)، فقد طورت فرنسا قوانينها الجنائية للتوافق مع المستجدات الإجرامية، حيث أصدرت أول قانون خاص بها (The First special law)، في عام (١٩٨٨) ، القانون رقم (١٩-٨٨) ، والذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لتلك الجرائم كما تم في عام (١٩٩٤)، تعديل قانون العقوبات لديها ليشمل

مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية، وقد أوكل هذا القانون إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب عمل التحريات وسماع الأقوال والشهود.

أما هولندا فقد قامت هي الأخرى بتعديل القوانين الخاصة بها للتوائم مع تلك الجرائم الحديثة ليكون في إمكانها التعامل معها ومحاولة السيطرة عليها، فقد قامت بتعديل القوانين الخاصة بها، ونصت في تلكم القوانين على أنه من حق القاضي ان يصدر أوامره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، ومتى كان هذا التصنت على قدر من الأهمية للكشف عن تلك الجريمة.

أما فنلدنا فهي الأخرى فقد تم تعديل القوانين الخاصة بها وأصبح للقاضي الحق في إصدار أوامره بمراقبة اتصالات الحاسب الآلي وتسجلها والتعامل معها إلا أن القانون قد أعطى ذلك المحقق بشرط إلا في مدة أقصاها ثلاثة أيام.

أما في اليابان فقد قامت هي الأخرى بسن القوانين الخاصة بها لتستوعب المستجدات الإجرامية المتمثلة في جرائم الإنترنت والحاسب الآلي وقد نصت تلك على أنه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إنشاء كلمة السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته كما أقرت في قانون خاص سنته عام (١٩٩١)، شرعية التصنت على شبكات الحاسب الآلي فقط إذا ما كان ذلك في مجال البحث عن الأدلة الخاصة بإحدى الجرائم الإلكترونية.

قامت دولة المجر هي الأخرى بدورها تماشياً مع الوضع الجديد، بسن قوانين خاصة بها لتجرم الجرائم الإلكترونية، وقد نصت تلك القوانين التي سنتها على كيفية التعامل مع مثل هذا النوع من الجرائم، وأيضاً كيفية التعامل مع المهتمين بإرتكاب الجرائم، وهي الإجراءات التي تسهل عمل الجهات المنوط بها مواجهة مثل تلك الجرائم والقبض على المتهمين بإرتكابها.

كذلك دولة بولندا قامت بسن قوانين خاصة بها وتلك القوانين التي سنتها تنص على أن للمتهم بارتكاب الجرائم الحق في عدم طبع أي سجلات خاصة بالحاسب الآلي أو إنشاء كلمات السر المستخدمة أو حتى الأكواد الخاصة بالبرامج، كما أنها تنص على حقوق أخرى بالنسبة للشهود في تلك الجرائم فهي تعطي الشاهد أيضاً الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى كان ذلك قد يؤدي إلى إدانته أو إدانة أي من أقاربه، بل أن تلك القوانين تذهب

إلى مدى أبعد من ذلك فتلك القوانين تنص على أن لا يقابل ذلك أي إجراء قسري قد يتخذ وتكون من نتائجه إدانة بالمتهم.(١٣)

ب- على المستوى العربي:

ليس هناك في العامل العربي ما يستحق الوقوف عنده كثيراً، فإنه للأسف الشديد لا توجد أي دولة عربية قد قامت بسن قوانين جديدة (New Laws)، خاصة بها أو حتى تحديث قوانينها الخاصة لتستوعب تلك المستجدات الإجرامية، فالدول العربية لا زالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي ، بينما نجد أن الدول العربية لا زالت لا تحرك ساكناً.

نجد مصر على سبيل المثال لا الحصر لم تعمل على سن قوانين جديدة خاصة بها في هذا المجال ولم تقم حتى بتعديل ما لديها من قوانين وإنما القانونيين في مصر يحاولون تطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعاً من الحماية الجنائية ضد الأفعال المشابهة بالأفعال المكونة لأركان الجريمة المعلوماتية ومن ذلك على سبيل المثال، اعتبر أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات ، كما تم تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض جرائم الإنترنت، وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية.(١٤)

يتضح مما سبق، أن البلاد العربية ليس فيها عملية لسن قوانين جديدة، ولا حتى تعديل لتلك القوانين لكي تستوعب الأحداث والمستجدات الجديدة الإجرامية ومنها جرائم تكنولوجيا المعلومات، وأن ما يوجد فيها هو عملية تطويع للقوانين السابقة ومحاولة إدخال الجرائم الإلكترونية تحت بعض نصوصها، ناسين أو متناسين طبيعة هذا النوع من الجرائم ، وكذلك حجم الخسائر المادية والنوعية التي تخلفها، وملابسات أو الغموض الذي يكتشف لحظة ارتكاب الجريمة الإلكترونية، وكذلك تناسوا النتائج المترتبة من جراء ارتكاب تلك الجرائم. وبذلك تؤكد الأمة العربية على تمسكها بالتخلف ولا بديل عنه والدليل على ذلك يؤكده رجال القانون العرب من خلال عدم التعديل في القوانين القديمة، ولا سن قوانين حديثة تتوافق ومعطيات العصر الجديد، عصر تكنولوجيا المعلومات.

أما في المملكة العربية السعودية ، فهي الأخرى لا تختلف عن بقية الدول العربية الأخرى، إلا أنها تنطلق أغلب كافة قوانينها من الشرعية الإسلامية، وقضية الجريمة والعقاب في الشريعة تتسم بوضع متميز بين سائر التقنيات الجنائية المقارنة، حيث عالجها الشارع الحكيم في إطار النظام القانوني الشامل المتكامل الذي يغطي كل جوانب الحياة ويصلح لك زمان ومكان. فالتجريم والعقاب في النظام الإسلامي يتوجه مباشرة إلى صيانة وحماية المصالح المعتبرة في الإسلام، وهي الدين والنسل والنفس والمال والعقل، وأي اعتداء على مصلحة من تلك المصالح يعتبر جريمة يعاقب فاعلها ويختلف بالطبع مقدار العقاب حسب جرامة الفعل الإجرامي.

لقد صدر في المملكة العربية السعودية نظام حماية حقوق المؤلف بالمرسوم الملكي برقم م/١١ في ١٤١٠/٥/١٩هـ، حيث توضح المادة الثالثة منه، الأنواع المشمولة بالحماية وورد في البند عاشراً: برامج الحاسب الآلي، وأوكل إلى وزارة الإعلام متابعة تنفيذ هذا القرار، حيث تم إنشاء إدارة متخصصة لهذا الغرض باسم "إدارة حقوق المؤلفين".

ومما تجدر الإشارة إليه أن عقوبة نسخ البرامج في السعودية تصل إلى إغلاق المحل المخالف (١٥) يوماً وتغريمه (١٠.٠٠٠) ريال مع مضاعفة هذه العقوبة في حالة تكرار المخالفة. (١٥)

بيد أن المشرع في المملكة العربية أغفل أم تغافل عن العديد من القضايا المعاصرة التي لم يصدر فيها شيء ولم تناقش مناقشة مستفيضة من قبل العلماء ولم تصدر فيها فتاوى على حد علم الباحثين ومن ضمن تلك القضايا السرقة التي تتم بواسطة الحاسب وهل يطبق عليها حد السرقة في الشريعة الإسلامية أم لا؟ بمعنى هل العقوبة التي تتخذ ضد مرتكب جريمة السرقة من الحاسب أو عن طريق الحاسب من العقوبات المقدرة أم غير المقدرة؟ وهل تنطبق على مرتكبها شروط إقامة حد السرقة؟ وهل حد القطع كاف أم لا بد أن يكون لها عقوبة أكبر من ذلك؟

أضف على ما سبق، ما الحكم في التقول على الأخرين وسبهم وشتمهم والإفتراء عليهم نشر أخبار وأقوال كاذبة عنهم وعن أعمالهم وصور مزيفة لهم باستخدام القص واللزق بسهولة، ناهيك عن نشر الرذيلة عنهم واتهامهم بالباطل والخوض في أعراضهم، علاوة على ذلك، ما الحكم فيمن ارتكب جريمة الحاسب تزييفه للنقود الورقية والوثائق وغيرها؟، حيث أصبحت المحاكاة والتقليد للعملة والوثائق أسهل عما كانت عليه في السابق. كذلك ما حكم الشريعة في المتطفلين/ المتسللين من المهرة من المخترقين الذين يتعمدون التخفي بمحاولة تفادي برامج الحماية الموجودة في حاسب الضحية أو مسح آثار جريمتهم لتحقيق أهدافهم؟، فما الحكم فيهم إذا تم التعرف عليهم؟(١٦)

كل تلك الأسئلة تحتاج إلى إجابات دقيقة وصريحة وواضحة من خلال سن قوانين جديدة تتناسب وطبيعة معطيات العصر الحاضر، فمسألة الاعتماد على القوانين السابقة ومحاولة تطويعها لمكافحة جرائم حديثة مثل جرائم تكنولوجيا المعلومات، وفي حقيقة الأمر لا نرى هناك ما يمنع الدول العربية من سن قوانين جديدة أو تعديل قوانين سابقة، وإن دلّ ذلك على شيء إنما يدل على تمسك العرب بالماضي ولا يمكنهم الدخول إلى العصر الجديد، الذي فرضت فيه العولمة العديد من الأمور فرضاً على أغلب المجتمعات ومنها المجتمع العربي، وجرائم تكنولوجيا المعلومات من معطيات العولمة.

رابعاً: التعاون الدولي:

بات مؤكداً أن جرائم تكنولوجيا المعلومات هي جرائم عابرة للحدود، أي أنها لا تتم وتنتهي في أراضي دولة بعينها، وعليه فالتعاون الدولي هو من أهم سبل مكافحة جرائم الإنترنت، وملاحقة مرتكبيها، فبغير التعاون الدولي يزداد معدل ارتكاب تلك الجرائم ويطمئن مرتكبوها من عدم إمكانية ملاحقتهم، إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تبيح القوانين السارية بها ما ارتكبوه من جرائم.

تعد المعاهدات الدولية التي تنضم إليها العديد من الدول هي النموذج الذي يكون هذا التعاون الدولي في ذلك المجال. ومثال ذلك أيضاً التعاون الدولي في مجال مكافحة الجريمة المنظمة، وقد بدأ هذا التعاون الدولي بمؤتمر الأمم المتحدة السابع والذي عقد عام (١٩٨٥)، لمنع الجريمة المنظمة، حيث اعتمد خطة عمل ميلانو والتي أوصت بعدة توصيات حيال التعامل مع الجريمة المنظمة والقضاء عليها.

يضاف على ذلك ، الاجتماع الإقليمي التحضيري والذي عقد عام (١٩٩٨)، والذي تم فيه إقرار المبادئ التوجيهية لمنع الجريمة المنظمة ومكافحتها، ثم تبعه المؤتمر الثامن لمنع الجريمة بفنزويلا عام (١٩٩٠)، فالمؤتمر الوزاري العالمي المعنى بالجريمة المنظمة عبر الوطنية في نابولي بإيطاليا عام (١٩٩٤)، والذي عبر عن إرادة المجتمع الدولي بتعزيز التعاون الدولي وإعطاؤه الأولوية لمكافحة الجريمة المنظمة.

كانت معاهدة المجلس الأوروبي حول جرائم الشبكات الإلكترونية التي أيدتها الولايات المتحدة بقوة هي أول خطوة رئيسة في هذا الاتجاه، ويمكن اعتبارها بداية لعملية وضع القواعد

والمعايير التي يتوقع مـن البلـدان المعنيـة أن تتبعهـا في نهايـة الأمـر في جهودهـا التـشريعية والتنظيميـة وتطبيـق القوانين.

يستند نهج هذه المعاهدة إلى اعتراف أساسي بضرورة قيام انسجام بين قوانين الدول قوانين الدول المعنيـة، وقـد تـم تحقيق التعاون الدولي في تطبيق القوانين من خلال سلسلة من معاهدات تسليم المجرمين والمساعدة القانونية المتبادلـة التي تمكن الحكومات من تبادل المعلومات والأدلة وبغية وضع هذه المعاهـدات قيـد التنفيـذ يفـترض عـادة وجـود مـا يعرف بازدواج العمل الإجرامي (أي أن تكون السلطات القضائية لكـلا الـدولتين تعتـبر ذلـك عمـلاً جرميـاً)، وعليـه يـتم تسهيل التعاون الدولي بدرجة كبيرة من خلال التلاقي على ما يمكـن اعتبـاره عمـلاً إجراميـاً بموجـب تـشريعات مختلـف البلدان المعنية فإن فرض قوانين مماثلة في مختلف الدول يزيد المخـاطر التـي تواجـه مرتكبـي جـرائم الإنترنـت، ويتجـه الأكثرية نحو معادلة هذه المخاطر في مختلف الدول المعنيـة، وفي الواقـع كلـما كانـت القـوانين أكـثر شـمولاً كلـما قلـت الملاذات الآمنة التي يستطيع المعتدون على الشبكات الإلكترونية العمل انطلاقاً منها بأمان.

إن الإنسجام ضروري بالنسبة إلى القوانين الأساسية كما بالنسبة إلى القـوانين الإجرائيـة وعـلى كافـة الـدول أن تعيـد تقييم ومراجعة قواعد الإثبات والتفيش وإلقاء القبض والتنصت الإلكتروني ومـا شـابه ذلـك لتـشمل المعلومـات الرقميـة وأنظمة الكمبيوتر الحديثة وأنظمة الاتصالات الحديثة والطبيعة العالمية لشبكة الإنترنـت، أمـا التنـسيق الأكـبر للقـوانين الإجرائية فيمكن أن يُسهل التعاون في التحقيقات التي تشمل سلطات قطاعية متعددة.

إضافة إلى القوانين الملائمة من المهم أيضاً أن تطور الحكومات وأجهـزة تطبيـق القـانون قـدراتها عـلى تطبيـق هـذه القوانين يحتاج ذلك إلى تطوير الخبرات في مجال الجريمة التي ترتكب عبر الشبكات الإلكترونية وتحقيـق مـشاركة فعالـة للمعلومات بين الدوائر داخل الدولة المعنية وبين مختلف الدول، يضاف إلى ذلك ضرورة تخطي هذه المـشاركة الأجهـزة التقليدية لتطبيق القوانين بحيث تشمل أجهزة الأمن القومي وأجهزة الاستخبارات كما أن مـن الأمـور الأساسـية تـشكيل وحدات متخصصة في تطبيق القانون للتعامل مع المسائل المتعلقة بهذا النوع من الجرائم على البلد المعني بإمكان هذه الوحدات أيضاً أن توفر أساساً للتعاون الدولي الرسمي وغير الرسمي المستند إلى شبكات ثقة بين مسؤولي تطبيق القوانين في مختلف البلدان ، ويمكن للتعاون في قضية معينة أو التعاون في لجان مشتركة مؤلفة من ممـثلي عـدد مـن الـدول أن يكون مفيداً جداً وهناك قضايا

كان فيها التعاون الدولي فعالاً للغاية، وبالفعل يمكن أن يولد التعاون الناجح تعاوناً مماثلاً في أماكن أخرى ويحقق المزيد من النجاح.

أما على المستوى العالم العربي، وضعت لجنة مكافحة الجرائم المنظمة مقترحات للعمل العربي في مكافحة الإرهاب والتي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة، وفي عام (١٩٩٦)، وافق المجلس في دورته الثالثة عشر على مدونة سلوك طواعية لمكافحة الإرهاب، ووافق عام (١٩٩٧)، في دورته الرابعة عشر على استراتيجية عربية لمكافحة الإرهاب، وفي عام (١٩٩٨)، أقر مجلس وزراء الداخلية والعدل العرب الاتفاقية العربية لمكافحة الإرهاب.

كان ذلك في مجال مكافحة الجرائم المنظمة، أما في مجال التعاون الدولي لمكافحة الإتجار في المخدرات فقد اهتمت كافة الدول بهذا الموضوع لما يسببه من أضرار على اقتصادياتها، وكذلك لما يسببه من إنهاك لثروتها البشرية. وعليه فقد كان هناك تعاوناً دولياً قوياً في مجال مكافحة الإتجار في المخدرات ومساعدة المدمنين على الإقلاع عن الإدمان.

أضف إلى ما سبق ، وعلى المستوى الدولي أيضاً ، عقدت اتفاقية مكافحة المخدرات عام (١٩٦١)، واتفاقية المؤثرات العقلية عام (١٩٧١)، واتفاقية الأمم المتحدة لمكافحة الإتجار في المخدرات والمؤثرات العقلية عام (١٩٨٨).

أما على المستوى العربي، فقد تم في عام (١٩٩٦) إقرار الاتفاقية العربية لمكافحة الإتجار في المخدرات والمؤثرات العقلية ، كما تم في عام (١٩٩٦) إقرار القانون العربي النموذجي الموحد للمخدرات.

عليه ، فإن لتفعيل التعاون الدولي لا بد من التركيز على أربع موضوعات رئيسة لا بد من العمل على تعظيم وجودها والأخذ بها وهي كالآتي:

١- الانضمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون والتنسيق بين الجهود التي تبذلها في مجال مكافحة الإنترنت.

٢- إدخال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلي ، أي تنفيذ ما تنص عليه تلك الاتفاقيات من إجراءات دون أي إبطاء.

٣- العمل على وجود أكبر قدر ممكن من التناسق والتطابق فيما بين قوانين الدول المختلفة والمتعلقة بمكافحة جرائم الإنترنت، فلا يكون الفعل الذي تم ارتكابه جريمة في بلد ما

وغير معاقب عليه في قانون بلد آخر، فمن هنا يجد المجرمون الملاذ الأمن الذي يلجؤن إليـه دون أي اعتبـار لما ارتكبوه من جرائم.

٤- تعاون جميع الدول في تسليم المطلوبين أمنياً إلى الدول التي تطالب بهم لارتكابهم جرائم الإنترنت (١٧)

أضف إلى ما سبق، أن مسؤولية المجتمع الواحد لم تعد الدولة المعنيـة بهـذا المجتمـع قـادرة عـلى توفيرهـا في زمـن العولمة، وعليه بات لزاماً على كل مجتمع من المجتمعـات، بـل كـل فـرد ومنظمـة التعـاون معـاً في سـبيل تحقيـق أمـن المواطن أولاً ومن ثم المجتمع فالدولة، انطلاقاً مـن قولـه تعـالى: +وتعـاونوا عـلى الـبر والتقـوى ولا تتعـاونوا عـلى الإثـم والعدوان-.

خامساً: اتحاد الشركات والكيانات الاقتصادية في مجال حماية أمنها الإلكتروني:

تعد الكيانات الاقتصادية من أهم الأهداف المحتملة لأي عمليات إجرامية تتم عبر الإنترنت، وغالباً ما يكون الهـدف من ارتكاب تلك الجرائم هو البحث عن أموال تلك الشركات الضخمة أو عما تخفيه من معلومات تريد الشركات الأخرى الحصول عليها في محاولة منها للتغلب على ما تعانيه من نقص في المعلومات التكنولوجية التي تـساعدها عـلى النهـوض تكنولوجيا وتصبح في عداد الشركات الاقتصادية الكبرى والمتقدمة اقتصادياً بما يعود عليها مـن فوائـد اقتـصادية ضـخمة، وعليه فغالباً ما تكون الشركات الاقتصادية هي الهدف السمين الذي يلهث وراءه مرتكبي جرائم الإنترنت.

يضاف إلى ذلك ، قد يكون الهدف من الجرائم التي تتعرض لها تلك الشركات الاقتصادية الضخمة هي الحصول على معلومات هامة عنها القيام بابتزازها والحصول منها على مبـالغ ماليـة في مقابـل عـدم نـشر مـا تـم الاسـتيلاء عليـه مـن معلومات في الغالب يكون نشرها ضاراً بالشركة ضرراً بالغاً.

بناءً على ذلك ، صار لزاماً على العديد مـن الكيانـات الاقتـصادية الهامـة في العـالم أن تتحـد مـع بعـضها الـبعض في محاولة منها للقيام ببناء حائط صد إلكتروني مضاد لهـا قـد تتعـرض لـه مـن هجـمات ومحـاولات اخـتراق وقرصـنة مـن محترفي ارتكاب جرائم الإنترنت ومكاسب تلك الكيانات الاقتصادية عظيمة من تعاونها مع بعضها الـبعض في هـذا الأمـر، منها:

١- إن التعاون الذي يتم بينها وبين الكيانات الاقتصادية الأخرى يوفر لها قدراً كبيراً من الأموال فيما لو كانت ستقوم ببناء هذا الحائط المضاد بمفردها، فعندها كانت ستتحمل بمفردها ما يتكلفه من أموال دون أي مساعدة من أي جهة خارجية.

٢- إن هذا الاتحاد يكون ائتلافا قوياً في مواجهة تلك الهجمات التتارية على تلك الكيانات، وبالتالي يجعلها أقوى عند مواجهة تلك الاختراقات وصدها وتعقب مرتكبيها.

٣- إن تعاون تلك الشركات وعدم تحمل أي منها للتكاليف بمفرده يجعلها تستطيع القيام ببناء حائط صد قوي ومنيع في مواجهة مرتكبي جرائم الإنترنت، وبالتالي يصعب كثيراً من فرص اختراقه والنفاذ إلى تلك الشركات.

فعليه نجد أن تعاون الكيانات الاقتصادية الكبرى في مجال مكافحة جرائم الإنترنت يساعد كثيراً على حماية أمنها من مخاطر التعرض لتلك الجرائم ويحافظ عليها من أي محاولات ابتزاز قد تتعرض لها إذا ما استطاع أي شخص النفاذ إلى معلوماتها والحصول عليها، فعندئذ سيكون عليها أن تدفع له الكثير من الأموال لمنعه من نشر معلوماتها السرية والتي قد تستفيد منها أي شركات منافسة لها في الأسواق العالمية أو التي قد تضر بالشركة ضرراً بليغاً إذا ما تم نشر تلك المعلومات.

سادساً: المعاهدات والقوانين الخاصة بحماية حق الملكية الفكرية:

مما لا شك أن حقوق الملكية الفكرية هي من أكثر الحقوق التي يتم انتهاكها يومياً على شبكة الإنترنت أو على كافة شبكات الاتصالات والمعلومات على مستوى العالم، وعليه فوجود معاهدات دولية تمنع تلك الانتهاكات وإصدار كل دولة قوانين خاصة بها تعمل على حماية حقوق الملكية الفكرية كل ذلك يؤدي إلى الحفاظ على تلك الحقوق من الانتهاك الذي يومياً دون أي رادع يحمي أصحاب تلك الحقوق.

من أهم المعاهدات الدولية التي تم إبرامها في مجال حماية حقوق الملكية الفكرية:

١- معاهدة برن لحماية المصنفات الأدبية والفنية:

تعد معاهدة برن والتي تم التوقيع عليها في عام (١٩٧١) في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف، وقد وقعت على هذه الاتفاقية (١٢٠) دولة، وتعد المادة التاسعة من

تلك الاتفاقية هي أساس في تلك الاتفاقية؛ لأنها تنص على منح أصحاب حقوق المؤلف حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان.

فضلاً عن ذلك تمنح اتفاقية برن صاحب حق المؤلف، الحق في أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه، وكذلك تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنياً أم أجنبياً.

٢- معاهدة تريبس.

معاهدة تريبس هي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطو عليها لاسيما مع انتشار عمليات السطو الإلكتروني على الأعمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية.

تلك الاتفاقية تم التوقيع عليها من قبل الدول الأعضاء بها عام (١٩٩٤)، وقد عالج موقعو الاتفاقية العامة للتعريفات والتجارة (الجات) حقوق الملكية الفكرية بتوقيع اتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (TRIPS)، فربطوا بذلك بين المعايير الدولية والمعايير المحلية، وتتضمن تلك الاتفاقية العديد من الإجراءات الهامة والفعالة لردع الاعتداءات على حقوق الملكية الفكرية، كما أنها ومن وجه أخرى تفرض على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع.(١٨)

سابعاً: التعرف على الوجوه:

مثلما لعبت تكنولوجيا المعلومات دوراً سلبياً تمثل في مساعدتها للمجرمين على ارتكاب الجرائم، لعبت في ذات الآن دوراً إيجابياً في متابعة ومكافحة تلك الجرائم، وقد يساعد التعرف على الوجوه باستخدام الكمبيوتر مستقبلاً في الحد من معدلات انتشار الجريمة فمثلاً تعتبر أجهزة الصرف الآلي مصدراً للعديد من عمليات الاحتيال، التي تقدر بملايين الدولارات في دول العالم المختلفة سنوياً، كما أن عمليات الاحتيال على نظام المساعدات الاجتماعية التي تقدمها الحكومة الأمريكية تقدر بعشرات البلايين من الدولارات سنوياً، كما يمكن القول : إن العديد من الصور الموجودة على رخص القيادة غير واضحة بما فيه الكفاية، وتشكل تحدياً للقدرات البشرية فيما يتعلق بتعرف صحة هذه الصورة ومطابقتها مع الوجوه الحقيقية.

لذلك كله ... فإن توظيف نظام التعرف على الوجوه باستخدام الكمبيوتر، سوف يسهم إسهاماً كبيراً في التخلص مع العديد من خروب النصب والاحتيال من خلال التثبت من حامل

بطاقة الصرف الآلي، أو هوية الشخص المستحق للمعونات من نظام المساعدات الاجتماعية، أو ضمان الإتقان الكافي لتحليل قاعدة بيانات كاملة من رخص السائقين بسرعة فائقة، وبشكل الذين يفقدون رخص القيادة في الحصول على بدل فاقد لها؟ دون إبراز أية أوراق أخرى لتحقيق الشخصية سوى وجوههم.

قد تطلبت المحاولات السابقة للتعرف على الوجوه باستخدام الكمبيوتر أجهزة قوية وغالية الثمن، لكنها كانت بطيئة في العادة وتعطي نتائج مغلوطة، إذ كان استخدام النظارات أو تغيير تصفيفة الشعر يؤدي إلى إرباك النظام والتغلب عليه. أما الآن، فباستخدام (فوتوبوك)، (Photo book)، وبوجود مجموعة من أدوات الكمبيوتر التفاعلية .. فإن يمكن استخدام النظام ليعرف أنواع متعددة من الصور؛ بما فيها الأشكال الهندسية والجداول الزخرفية. ومن هنا، قد تكون قدرة تعرف الوجوه في نظام (فوتولوك) إحدى أكثر ميزاته، حيث يمكنه البحث عن كل الوجوه التي تطابق وجهاً مستهدفاً في قاعدة بيانات ، تتألف من آلاف صور الوجوه في أقل من ثانية واحدة.

يصعب عادة خداع نظام (فوتوبوك) باستخدام بعض التعقيدات، مثل ارتداء القبعات أو النظارات، بالإضافة إلى أنه قادر على التعامل مع تعبيرات الوجوه المختلفة، والتغيرات في الإضاءة، وإيماءة الرأس وشعر الوجه، إلا أن هذا لا يمنع أن الجهود الكبيرة للخداع يمكن أن تنجح مع الكمبيوتر كما تنجح في خداع الإنسان. وعلى الرغم من ذلك، فبالنسبة لمعظم تطبيقات التعرف على الوجوه ذات الطابع التجاري .. فإن المطلوب هو تعرف شخص معين لاستخدام بطاقة الصرف الآلي، أو الدخول إلى مبنى، أو استخراج رخصة قيادة أو جواز سفر، أو صرف المساعدات الاجتماعية. ولذلك.. فلن تكون ثمة مشكلة عند الطلب من هؤلاء الأشخاص اتخاذ وضع معين أو نزع نظاراتهم أو قبعاتهم، عند التقاط صورهم لاستخدامها في نظام تعرف الوجوه باستخدام الكمبيوتر.

بينما يتذكر الإنسان الوجوه التي يصادفها باستخدام ملامح خاصة، مثل شكل العينين أو طول الأنف أو استدارة الفم ... فإن نظام (فوتوبوك) يتجنب هذه الملامح الواضحة، ويتم العمل من خلاله وفقاً للمبادئ الاساسية لنظرية المعلومات في تذكر الوجوه، حيث يقوم البرنامج أولاً بتقسيم كل وجه إلى منطقتين ثنائيتي الأبعاد، إحدهما فاتحة ، والأخرى داكنة، وبعد ذلك يحدد البرنامج أفضل السمات لتمييز وجه عن الآخر، ويطلق الباحثون على سمات التمييز هذه (الوجوه

المميزة). وبعد ذلك يقوم البرنامج بتصوير كل وجه من الوجوه كخليط من الخصائص، حيث يُخزن صورة الخصائص لكل وجه في قاعدة البيانات.

كيف يتعرف فوتوبوك على الوجوه؟

يقوم فوتوبوك بإنشاء مجموعة مرجعية لخصائص الوجوه، عن طريق تحليل كافة الوجوه في قاعدة البيانات. وبدلاً من مطابقة الميزان التي يتمكن الإنسان، مثل لون الشعر أو شكل الأنف، يستخدم فوتوبوك الخصائص الأساسية لكل صورة من صور الوجه، التي تسمى الوجوه، التي تسمى الوجوه المميزة لتوفير الأنماط، التي يمكن استعمالها في مقارنة وجه مستهدف. ولتعرف صورة مستهدف لوجه ما، يقوم البرنامج بقارنة الوجه في هذه الصورة والتي تصل إلى أربعين خاصية في الحالات النموذجية، مع الوجوه المميزة الموجودة في قاعدة البيانات، ثم يحدد الوجوه التي تطابق صورتها تماماً الوجوه المستهدفة، وفي حالة تحديد شروط للتعرف تستوفيها المطابقات، يكون الوجه المستهدف قد تم تعرفه، أما عن عدم تحديد شروط التعرف، فيمكن للبرنامج أن يعرض الوجوه المطابقة حسب ترتيب مطابقتها، ومن ثم يمكن للمستخدم تعرف الوجه المستهدف يدوياً.

بالإضافة إلى ذلك فقد صممت إحدى الشركات بجنوب انجلترا آلة تصوير يمكنها تعرف الوجوه المتنكرة وتحديد الشخصية بالضبط. وتلتقط آلة التصوير (٢٥٠) صورة في الثانية ليتم بعد ذلك عرض الصور على شاشة بتخزين كل المعلومات والتفاصيل ومميزات أجسام الأشخاص المشتبه فيهم، يمكن لآلة التصوير إظهار الوجه الحقيقي في ثوانٍ معدودة.

بدا بالفعل استخدام تطبيقات التعرف على الوجوه من قبل بعض أجهزة الشرطة في العالم، فعلى سبيل المثال، بدأ البوليس البريطاني في أواسط أتوبر (١٩٨٨)، للمرة الأولى في اختبار جهاز كمبيوتر يتعرف بتعرف خريطة الوجه، ويسمح بتعرف وجوه المجرمين والمشتبه فيهم والإرهابين، من خلال المقارنة بين الصورة المخزنة به والصور التي تلتقطها كاميرات الشوارع والمحال وغيرها، وأشار البوليس إلى أن هذا الكمبيوتر سوف يتم استخدامه لملاحقة اللصوص والمتهمين بالسطو على المنازل والمباني وسارقي السلع من المحال، كما أنه من المتوقع أن يمتد دوره إلى ملاحقة القتلة المطلوبين للعدالة والإرهابيين.

كما أنشأت شبكة (BBC) الإخبارية البريطانية موقعاً على الإنترنت بعنوان (مراقبة الجريمة) "Crimewath" ، ويحتوي هذا الوقع على قائمة لصور وتهم عدد من المتهمين المطلوب القبض عليهم.

وقد ساعد هذا الموقع البوليس الألماني في القبض على أحد المطلوبين للعدالة في بريطانيا، وقد كانت تهمته هي استخدام بطاقات اعتماد مسروقة، وقد تم تحديد مكان تواجد المتهم ، من خلال نشر صورة له على الموقع المشار إليه، فتم القبض عليه على الفور.

ثامناً: القياسات الحيوية لبصمات الأصابع والصوت وقاع العين:

توجد بعض القياسات الحيوية التي يمكنها اكتشاف هوية الأشخاص ، حيث إنه من المفترض أن هذه القياسات لا تتطابق بين شخصين مختلفين ، ومن بين هذه القياسات: تعرف بصمات الأصابع والصوت وقاع العين، ويفيد ذلك في كشف شخصية المجرم.

تتميز أساليب القياس الحيوي بأنها دقيقة وسريعة في الوقت ذاته، حتى أنه في بعض الولايات المتحدة الأمريكية تعتمد آلة صرف الشيكات المصرفية على فحص الوجه للتأكد من شخصية آلاف العملاء، الذي يترددون عليها يومياً من أجل معاملاتهم المالية. ومن الواضح أن هذه الأساليب المتطورة تكنولوجيا لتعرف الأشخاص تتناسب تماماً مع عصر تطورت فيه أساليب التزوير والتلاعب في البيانات الشخصية، بما في ذلك تلك البيانات المخزنة في ذاكرة أجهزة الكمبيوتر، وتعتبر البصمة كما هو معروف للجميع خاصية لكل شخص، ولا يمكن أن تتشابه بصمة شخص مع شخص آخر ، لذلك فإنها تُستخدم في التعرف على الشخص، ولكن عملية المقارنة بين بصمة وأخرى قد تستغرق وقتاً طويلاً، خاصة إذا كان المطلوب مقارنة البصمة مع عدة مئات من الآلاف من البصمات.

لتسهيل هذه العملية، يتم تخزين بصمات المجرمين أولاً في قاعدة بيانات، وقد تُخزن بعد ذلك بصمات الناس جميعاً مع بياناتهم الشخصية، وهذه البصمات تخزن في هيئة صورة باستخدام أجهزة المسح الضوئي (scanner) وعند الحصول على بصمات مجرم ما، يتم إدخال هذه البصمة إلى الكمبيوتر عن طريق جهاز المسح الضوئي الملحق بالكمبيوتر، الذي يقوم بعملية المقارنة واستخراج البصمة المشابهة بسرعة كبيرة.

وهكذا ... فإنه من الممكن أن تتاح قاعدة بيانات عن البصمات لجميع الجهات الأمنية، ويمكن لأية جهة في أي مكان داخل الدولة استخدامها في الحصول على المعلومات المطلوبة.

اخترعت من أجل هذا إحدى الشركات اليابانية جهازاً لمضاهاة البصمات، وهو الأصغر والأسرع في العالم لتحقيق الشخصية من خلال بصمات الأصابع ، فالبصمة التي يتم البحث عن

صاحبها، توضع إلكترونياً على شاشة صغيرة، ويضع المتهم إصبعه على جهاز ماسح ، فتظهر بصمته إلى جوارها ، لتجرى المطابقة بين البصمتين في نصف ثانية، بدرجة دقة تصل على (٩٩%).

ثبت كذلك علمياً أن قاع العين لأي شخص يحمل معلومات تخصه وحده، وكأنها بصمة من قاع العين، ولذلك فإن هذه المعلومات أيضاً تستخدم في تحديد هوية الشخص في حالة الدخول على أماكن حساسية مثل قاعدة حربية أو بنك، أو ما شابه ذلك، عن طريق وضع آلة تصوير متصلة بجهاز كمبيوتر، تخزن فيه صورة قاع العين للأشخاص المسموح لهم بالدخول، بالإضافة إلى كارت المرور حتى إذا استخدم شخص بطاقة شخص آخر يستوقفه الكمبيوتر، ويتم القبض عليه.

كما أن البصمة الصوتية تستخدم في بعض البنوك مثل التوقيع تماماً، من خلال أنظمة التعرف الصوتي (Vocie Recognition systems) التي شهدت قفزات هائلة في الآونة الأخيرة. وعلى الرغم من أن تقدم تقنيات تعرف الصوت وتوسعها بطيء نسبياً ، إلا أنه يسير بخطى واثقة ، حيث تجد هذه التقنيات في الوقت الحالي استخدامات ذات مغزى في تطبيقات جديدة غير تطبيقات الإملاء الصوتي، التي اعتدنا عليها فيما يتعلق بهذه التقنية، وأحد هذه التطبيقات هو التعرف على المتكلم (Speaker recognition)، والتي يتعرف الكمبيوتر بواسطتها البصمة الصوتية الخاصة بشخص ما.

يمكن للبصمة الصوتية أن تتحكم في الوصول إلى جهاز الكمبيوتر الشخصي، أو الرجوع إلى البيانات الشخصية، عند التوقف في أحد المتاجر الإلكترونية على شبكة الويب لشراء بعض الحاجات. وبذلك يمكن اعتبار البصمة الصوتية نوعاً من أنواع الهوية الشخصية، الذي لا يمكن للفرد أن يفقده ، إلا إذا كان مصاباً بالتهاب اللوزتين.

بدأ الباحثون في شركة (IBM) في تطوير هذه التقنية التي تمكن الكمبيوتر من فهم الصوت البشري، وعرض (ستيفان مايس) الباحث في مجموعة تقنيات اللغات البشرية في مختبر توماس واطسون التابع لشركة (IBM) حديثاً، أحد النتائج الطيبة لهذه الجهود ، وكانت عبارة عن تقنية (voiceprint) التي تستطيع التعرف على المتكلم ، بناءً على أي عدد من الكلمات الملفوظة بأية لغة.

وفي أثناء التسجيل، يبنى البرنامج نموذجاً لهندسة القناة الصوتية بين فتحة الحنجرة والفم، ويُحسب على أساس ذلك طنين الصوت المرتبط مع التجويف الحلقي للإنسان؛ ولذلك فإن هذا

النظام يعمل عن طريق مطابقة الخصائص الصوتية وليس الكلمات، وعلى الرغم من ذلك، فالهوية الصوتية لم تصل بعد إلى درجة الثقة التي نوليها لبصمات الأصابع.

يعد من الوسائل الحديثة في التعرف على الشخص ، استخدام الحامض النووي للخلية (DNA) من خلال أية نقطة دم توجد في مكان الجريمة، ومقارنتها بالحامض النووي للأشخاص المشتبه فيهم، ولا شك أن كل هذه الوسائل وغيرها تجعل من التكنولوجيا عاملاً مهماً في الحفاظ على الأمن في المجتمعات المختلفة.

يذهب بعضهم على ان استخدام بعض أنظمة التعرف على الوجوه مثل نظام (تروفيس) (Trueface)، والذي طورته مؤسسة (ميروز) بولاية ماساشوستيس الأمريكية يعتبر حلاً أفضل لسرية القياسات الحيوية، بالمقارنة باستخدام أنظمة بصمات الأصابع أو الصوت أو قاع العين، وذلك أنه إلى جانب تفوق هذا النظام على أنظمة القياسات الحيوية الأخرى كافة بنسب تزيد عن (٩٨%) فإن نظام (تروفيس) وتطبيقات تعرف الوجوه باستخدام الكمبيوتر تعتبر غير تفاعلية.(١٩)

تاسعاً: مكافحة التزييف والتزوير بالكمبيوتر:

لعبت تكنولوجيا المعلومات دوراً مهماً ولكنه سلبيٌ في مجال ارتكاب الجرائم التكنولوجية، والتي عادة ترتكب عن بعد، إلا أن هذه التكنولوجيا تلعب الدور ذاته، بل ويعد أهم منه، ويتجسد في مكافحة تلك الجرائم، ومنها جريمة التزييف والتزوير، لا سيما في مجال الأوراق النقدية التي طالما تضايق واشتكى الناس من وجود مبالغ طائلة موجودة في الأسواق ويتعامل فيها الناس، ولكنهم لا يعرفون إنها مزورة أو مزيفة، ويتم تأمين تلك الأوراق النقدية من خلال ثلاث عناصر رئيسة هي:

أ- نوع الورق:

إن الورق الخام المستخدم في طباعة العملات الورقية هو نتاج صناعة متطورة جداً وتكنولوجيا مكلفة ، وتتطلب خبرات متميزة واستثمارات كبيرة وحالياً، تعتبر إنجلترا وفرنسا من المصادر الأساسية لهذه النوعية من الورق ، وتقوم لجنة بتحديد المواصفات والقياسات الخاصة بورق البنكوت.

من العناصر المهمة في اختيار الورق الخام: مراعاة درجة توافقه مع درجة الحرارة والرطوبة التي يُطبع فيها، كما يجب مراعاة توافر الوسائل التأمينية المطلوبة في مرحلة تصنيع الورق نفسه، وأهم هذه الوسائل : العلامات المائية وشريط الأمان، فهذه العلامات يتم وضعها في أثناء عملية

تضيع الورق، وشريط الأمان له إشعاعات معينة يستطيع أي شخص أن يراها. كما يُراعى أيضاً أن يحوي الورق بعض الوسائل التأمينية للخبراء، كأن يوجد على سطح الورق شعيرات غير مرئية موزعة على سطح الورقة، ولها إشعاعات معينة لا تُرى بالعين المجردة.

ب- أحبار الطباعة:

إن الأحبار التي تُستخدم في طباعة أوراق النقد هي أحبار خاصة ، ولها سوق خاص، وهي تعتبر ذات صفة تأمينية. وهذه الأحبار ثابتة ولا تتأثر بالماء ، وحتى إذا وضعت نقدية في الماء فلن تتغير الأحبار، وبعد ان يجف الماء تعود الورقة إلى طبيعتها.

ج- التصميم:

إن التصميم عنصر مهم في الورقة النقدية، وقديماً كان الاهتمام ينصّب على نوع الورق والأحبار كوسيلتين من وسائل تأمين أوراق النقد، لكن الآن يتم التركيز على أهمية التصميم الذي يزيد من درجة تأمين أوراق النقد، بحيث يصعب تزويدها، ويظهر ذلك في الورقة فئة الخمسين جنيهاً والمائة جنيه، على سبيل المثال لا الحصر، هذا علاوة على شكلها الجمالي والطابع التاريخي الخاص الذي يضفيه على شكل الورقة لمكافحة تزوير المستندات وتزييف النقد.. توجد في العالم العربي والأجنبي دوائر تهتم بالأبحاث ذات العلاقة بموضوعي التزوير والتزييف، وهذه الدوائر لها أهميتها الكبيرة من الناحية الأمنية أو المالية المتعلقة بالأفراد. وفي الماضي كان يتم الاستعانة بخبراء أو المالية المتعلقة بالأفراد، وفي الماضي كان يتم الاستعانة بخبراء خطوط أو رسوم لاكتشاف تزوير أوراق النقد، أما اليوم فتوجد أجهزة أكثر تطوراً لتحليل ورقة النقد واكتشاف تزييفها.

إن وسائل التزوير لا تقف عند حدود بلد معين، وإنما تمتد لتشمل جميع دول العالم. وتعاني العملات العالمية المختلفة من التزوير والتقليد ، ولهذا فإنه يوجد تعاون أمني بين العديد من الدول المختلفة (٢٠) وسهلت تكنولوجيا المعلومات هذا التعاون، لاسيما الانترنت من أجل مكافحة الجرائم وخاصة تلك التي ترتكب بوساطة تكنولوجيا المعلومات، ومنها تزوير الأوراق الرسمية النقدية وغير النقدية.

عاشراً: تأمين الشبكات على نحو يمنع من اختراقها:

تحاول كل من المؤسسات الحكومية والشركات والمؤسسات الخاصة ، قدر الإمكان عمل شيئاً ما، يحد أو يقلل إلى حدٍ بعيد من اختراق مواقعها والشبكات المرتبطة بالإنترنت عن طريق

كمبيوتراتها. وتأتي تلك المحاولة من باب تأمين الشبكات العائدة لتلك المؤسسات بمثابة وسيلة تحد – إن لم تمنع مطلقاً– من عملية الاختراق لهذه الشبكات، ومن ثم فهي تؤدي بطريقة غير مباشرة إلى منع الكبار والصغار ، من محاولة اختراق تلك الشبكات، وبالتالي ربما تصبح هواية يمارسها هؤلاء وتقودهم في نهاية المطاف ليس إلى السرقة والتدمير فحسب ، بل التجسس الذي ربما يؤدي إلى نشوب حرب معلوماتية .

يقول خبراء الكمبيوتر: إن مقولة – الوقاية خير من العلاج – لا يمكن تطبيقها بدقة في مجال جرائم الإنترنت أو الفضاء الإلكتروني، ومع ذلك فإنه من غير الصحيح أن يترك الفرد منزله غير مغلق عند ذهابه إلى العمل صباحاً، ومن غير الصحيح أيضاً أن يترك الفرد نطاقه أو فضاءه المعلوماتي دون حماية بحيث يسهل الوصول إليه.

الحقيقة أن تأمين الشبكات له طرق عديدة منها:

١- جدار النار = Five walls:

هو عبارة عن مجموعة من البرمجيات والأجهزة التي يتم إعدادها لتحتل الحدود الفاصلة بين شبكتنا والشبكة التي نريد أن نحمي أو نقي حواسيب شبكتنا منها، وهي غالباً ما تكون شبكة الإنترنت.

الهدف من جدار النار: هو التغلب على أكبر قدر ممكن من الثغرات الأمنية من خلال بناء قناة اتصال توجه إليها المراسلات والمعلومات المتبادلة مع شبكة الإنترنت لمراقبتها والسيطرة على خروجها أو دخولها من وإلى شبكتنا. فقد يمنع الجدار كل (أو جزء) حركة المرور من شبكتنا باتجاه خدمات الإنترنت باستثناء البريد الإلكتروني، أو يستخدم جدار النار لمنع الوصول على المواقع المشبوهة(٢١).

بشكل عام يمكن القول: إن جدران النار هي عبارة عن برامج تقوم بصد محاولات الاختراق أو الهجوم الوافد من شبكة الإنترنت لتهديد الشبكة الداخلية أو النظام المعلوماتي، وتشبه برامج جدران النار حرس الحدود على الساحل، حيث تزود الشبكات بحماية جيدة عن طريق التأكد من شرعية كل شخص يود زيارة الشبكة المحمية دخولاً أو خروجاً دون أن يكون مصرحاً له بذلك.

يتم استخدام برمجيات جدار النار عند الأماكن التي تتلاقى فيها الشبكة الداخلية للشركة أو المؤسسة، مع شبكة الإنترنت العالمية، ويمكن القول بصفة عامة: إنه كلما زاد عدد خدمات

الإنترنت التي يسمح بها لمستخدمي الشبكة في المؤسسة المحلية، تزداد الخطورة من الدخول إلى شبكة الإنترنت العالمية، ولذلك تأتي وظيفة جدران النار في هذه الحالة، ويكون هدفها حماية المناطق الهامة من الشبكة الداخلية للمؤسسة الخاصة أو العامة.

توجد برامج عديدة لجدران النار من ذلك برنامج شبكة (DAN) والذي يتضمن مزايا أمنية عديدة عبارة عن برامج جدران النار (Firewalls) ، ومزودات بروكسي (Proxy servers) التي تحتفظ بصفحات الشبكة للويب على القرص الصلب، ومرشحات عناوين (arifilters).

فيما يخص مزودات بروكسي فهي تشبه الشاحنات العسكرية الخاصة بالتموين، والتي تجلب البضائع ، وهي في هذه الحالة صفحات الشبكة الخارجية، حيث يعاد توزيعها داخلياً، وتساعد عملية التوزيع الداخلي على خفض حركة المرور عبر بوابة الدخول إلى الشبكة المحلية، لأنها تلغي الحاجة إلى استدعاء البيانات مرة ثانية من مواقعها على شبكة الإنترنت، إذ سبق استدعائها وحفظها على القرص الصلب في الشبكة المحلية، وتستخدم مزودات بروكسي كذلك لمنع دخول البيانات الوافدة من إنترنت على الحاسب الآلي بالشبكة المحلية ، بصفة جزئية أو كلية.

أما مرشحات (URI)، فهي ببساطة عبارة عن فلتر يمنع مستخدمي الشبكة من الدخول إلى مواقع معينة على شبكة الانترنت، وبالتالي تعطي صاحب الشبكة أو مالكها الحق في التحكم في مستخدمي الشبكة أن يدخلوا أم لا على مواقع معينة غير مرغوب فيها على الشبكة، ولعل هذه الميزة من الأهمية بمكان فيما يتعلق بتصفح الطفل أو الحدث للإنترنت بطريقة آمنة ، بحيث لا يتسلل إلى المواقع الإباحية أو تلك التي يحصل منها على خبرات ضارة.

٢- **التشفير**= Ciphering: من طرق تحصين الشبكات الداخلية كذلك من الاختراق عملية التشفير، والتشفير يعني تحويل البيانات المكتوبة إلى أرقام أو رموز لا يمكن حلها إلا بالنسبة لمن يمتلك شيفرة حل هذه الرموز والأرقام، وتستخدم عملية التشفير في تداول النقود والبيانات عبر الشبكة في التجارة، وفي تداول غيرها من البيانات التي تتعلق بالأمن القومي، وهناك برامج تشفير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلي.

لمنع ومكافحة الجريمة أيضاً وقامت إحدى شركات المعلوماتية بتصميم برنامج هدفه الحيلولة دون دخول الأطفال إلى المواقع غير الناسبة لهم لاسيما وأن الجناة يقابلون الأطفال من

خلال غرف الدردشة، ويوجد كذلك في أسواق الكمبيوتر في الوقت الحالي برامج تمكن الآباء من التحكم في استخدام أطفالهم للإنترنت.(٢٢)

مكونات جدار النار:

يعد جدار النار من أهم وأقوى نظم الحماية التي يمكن أن تطبقها شبكة خاصة في حماية حواسيبها ومستفيديها من مخاطر الاتصال مع الشبكات الأخرى وخاصة شبكة الانترنت ومن المكونات الأساسية لجدار النار:

١- **السياسات الأمنية: Security Policy:**

يقصد بالسياسة الأمنية مجموعة القواعد الأمنية الواجب تطبيقها من قبل المؤسسة الراغبة بحماية شبكتها عند ربطها بالانترنت وتعريف الإجراءات الواجب اتخاذها لمنع الإخلال بأمن الشبكة، بالإضافة إلى الإجراءات المطلوب تنفيذها عند اكتشاف ثغرة أمنية معينة في النظام.

تقسم سياسة الحماية والأمن إلى مستويين:

الأول: يسمى بسياسة الدخول إلى الخدمات (Seyvice Access policy) يتم فيه تعريف الخدمات والجهات الخارجية المسموح لها بالدخول إلى شبكة المؤسسة استخدام بعض خدماتها أو السماح لمستثمري الشبكة بالاتصال مع هذه الجهات الخارجية واستثمار ما لديهم من خدمات. إضافة إلى تحديد الجهات والخدمات التي لا يسمح لحواسيب الشبكة الداخلية بالوصول إليها والتعامل معها.

الثاني: وهو المستوى الذي يهتم بكيفة تطبيق القواعد المحددة في المستوى، حيث يستخدم أحد المبداين المتضادين التالين في سياسة تطبيق القواعد الأمنية:

(كل ما لم يذكر بوضوح أنه مسموح فهو ممنوع)

أي فرض سياسة المنع العام لجميع الخدمات، ومن ثم السماح بمرور الخدمات التي تعطى لها السماحات.

(كل ما لم يذكر بوضوح أنه ممنوع فهو مسموح)

أي إعطاء السماح بمرور جميع الخدمات ومن ثم نع المرور للخدمات التي يرد إعلان بمنعها.

تعتبر القاعدة الأولى أكثر أمناً من الثانية.

٢- **مرشحات الرزم = Packet Filtering:**

المقصود بترشيح الرزم حماية الشبكات الداخلية للبلدان والشركات من الثغرات الأمنية الناتجة عن بنية بروتوكلات الاتصالات المستخدمة في شبكة الإنترنت من خلال مراقبة رزم البيانات القادمة والخارجة من الشبكة العالمية وإليها من هذه الشبكات الداخلية.

برمجيات الترشيح المسؤولة عن تأمين مستوى جيد من السرية غالباً ما تكون جزء من برمجيات موجهات المسارات التي يجب أن تسلكها هذه الرزم مع مراعاة عدم حصول تأخير لنقل المعومات أو التأثير في سرعة وفعالية الشبكة أو خلق صعوبات للمستفيدين في استغلال خدمات الشبكة.

تتم عملية الترشيح لبعض أو جميع الحقول التالية في بنية البروتوكول، (IP) ، (Internet Protocol):

١- حقل عنوان الجهة المرسلة.

٢- حقل عنوان الجهة المستقبلة.

أما في بنية البروتوكول " Transmission contral protocol) فهي تم على الحقول الآتية:

١- حقل عنوان بوابة المصدر.

٢- حقل عنوان بوابة الجهة المستقبلة.

إجراءات مرشحات الرزم:

معظم مرشحات الرزم تعمل حسب الطريقة الآتية:

١- تخزن قواعد الحماية في مرشد المسار بتحديد البوابات والعناوين المسموح بها، وتلك التي لا يسمح بالتعامل معها وذلك حسب سياسة حماية المطبقة.

٢- عند وصول رزمة البيانات إلى بوابة مرشد المسار فإنه يتم اختبار حقول ترويسة الرزم.

٣- إذا نتج من هذا الاختبار أن أحد قواعد الحماية تمنع إرسال أو استقبال هذه الرزمة فإنه لا يتم السماح لهذه الرزمة بالعبور.

٤- إذا كانت هذه القواعد تسمح بالإرسال أو الاستقبال لهذه الرزمة فإنها تعطى الأذن بمتابعة طريقها إلى العنوان المحدد والذي على أساسه تتم عملية أعطاء السماح أو رفضه.

٣- بوابات التطبيقات = Application Gateways:

تسمح مرشحات الرزم أو تمنع التعامل مع عنوان عقدة معينة من الشبكة ولكنها لا تستطيع التحكم بسماحات الدخول إلى التطبيقات المتواجدة على الحواسيب واستخدامها وهذه التطبيقات هي البرامج والخدمات الشبكية التي تساعد المستثمر على الدخول إلى حواسيب أخرى في الشبكة أو تمكنه من نقل أو تصفح المعلومات الموجودة في بعض الملفات Servers في شبكة الإنترنت.

مرشح الرزم الذي يعطي إذناً لجهة معينة فإن هذه الجهة يمكنها التعامل مع جميع الخدمات والبرمجيات المتوفرة على الشبكة الداخلية، وهذا قد لا يتوافق مع سياسة الحماية المتبعة في الشبكة مما يسبب خطراً على أمن هذه الشبكة لذلك فلا بد من وجود وسيلة للتحكم بعمليات الوصول إلى هذه الخدمات واستخدامها.

تتم عملية الحماية لهذه التطبيقات بواسطة مجموعة من البرمجيات التي تتولى مراقبة عمليات الدخول إلى تلك التطبيقات. حيث تشكل هذه البرمجيات حاجزاً يعبره من خلاله المستفيد إلى التطبيق بعد التأكد من هويته وهل يمتلك حق الاستخدام لهذه الخدمة أم لا ؟، حيث لكل خدمة برنامج حماية خاص يسمى البرنامج الوسيط (Proxy).

يخصص عادة حاسوب خاص توضع فيه مجموعة برمجيات حماية التطبيقات يوضع في مدخل الشبكة المطلوب حمايتها ويسمى هذا الحاسوب اسم عبور التطبيقات، (Application Gateway).

أما الخدمات الواجب حمايتها من عبث المخربين فهي عديدة، منها:

١- خدمة بروتوكول تبادل الملفات.

٢- خدمة الولوج من بعد.

٣- خدمة البريد الإلكتروني.

٤- خدمة نقل الملفات.

٥- خدمة أسماء المناطق.

إجراءات بوابات التطبيقات:

معظم بوابات التطبيقات تعمل بالطريقة الآتية:

١- يتصل المستفيد ببوابة العبور ويطلب اسم الحاسوب الداخلي الخاص بالشبكة المحمية.

٢- تقوم البوابة باختبار عنوان مصدر الرسالة وتقرر منع الاتصال أو متابعته، وذلك حسب قواعد العبور التي تمتلكها.

٣- في بعض الأحيان تطلب بوابة العبور من المستفيد ادخال كلمة المرور الخاصة بعبور البوابة .

٤- بعد التأكد من امتلاك المستفيد للسماح المطلوب يقوم برنامج حماية التطبيق بوصل بوابة العبور بالحاسوب الذي يمتلك التطبيق.

٥- يتولى برنامج الحماية بنقل البيانات ما بين الاتصالين القائمين.

- ما بين المستفيد وبوابة العبور.
- ما بين بوابة العبور والحاسوب الداخلي الذي يمتلك التطبيق.

٦- كل عمليات التخاطب ما بين المستفيد والتطبيق تتم من خلال وبواسطة بوابة العبور.(٢٣)

إمكانيات ومحددات جدار النار:

يقوم جدار النار بأكثر من مجرد حماية الشبكة الخاصة من الدخلاء، فهو يستطيع أن يوفر معلومات حيوية عن النشاط المرتبط بالنظام، فهو يقوم بما يلي:

١) يتحكم بعملية الاتصال بأنظمة الشبكات الخاصة.

٢) يضع إدارة أمن الشبكة في أيدي مجموعة قليلة.

٣) يمكنه أن يزيد من الخصوصية (Privecy)، عن طريق إخفاء العناوين الخاصة بمستفيدين يستخدمون الشبكة.

٤) تسجيل الحركة على الشبكة لأغراض التدقيق، وإصدار الفواتير.

٥) إمكانية تقديم تقارير عن التحركات المشبوهة.

٦) إمكانية العمل مع برامج الكشف عن الفيروسات.

أما محددات جدار النار فهي تشمل:

١) يمكن أن تبدو الحماية التي يحققها مبالغ بها، وتحول دون الوصول إلى بعض الخدمات الضرورية وغير الضارة.

٢) لا يمكنه منع المشكلات التي تحدث داخل الشبكة.

٣) يمكن أن يتسبب باختناقات مرورية، بسبب الحجم الكبير لحركة البيانات داخل الشبكة.

٤) يمثل نقطة ارتكاز وحيدة فإذا أصابها العطل فلا يمكن لأي شيء من الدخول أو الخروج(٢٤).

إحدى عشر: الملقمات الوسيطة (proxy server):

بسبب المخاطر الأمنية المحتملة من ارتباط الشركة بشبكة الإنترنت، فإن هذه الشركات تسعى لتخصيص جهاز يسمى (proxy server)، الذي يؤدي دور البوابة الخارجية (gateway) لشبكة هذه الشركة إلى شبكة الإنترنت يقوم هذا الجهاز بتصفية (filtters)، طلبات المغادرة عبر هذه البوابة من مستفيدين الشبكة الخاصة بالشركة باتجاه شبكة الإنترنت، هذه التصفية تكون قائمة على أساس تقييد عمليات الوصول لهؤلاء المستفيدين إلى مواقع (Sites) معينة من الإنترنت والحيلولة دون الوصول إليها أو منع الوصول في أوقات معينة أو السماح للبعض بالوصول ومنع الآخرين، ويتم ذلك وفق سياسات معينة تحدد مسبقاً أثناء تنصيب هذا الملقم الخاص بدلاً من طلب صفحات الويب، خدمة البريد الإلكتروني والخدمات الأخرى بشكل مباشر من قبل أحد حواسيب الشبكة، فإن هذا الحاسوب يطلب الخدمة من الملقم الوسيط، عندها يقوم هذا الملقم بتوجيه الطلبات إلى الملقمات الفعلية على الإنترنت بالنيابة عن حواسيب الشبكة، وعند استجابة الملقمات المستهدفة لهذه الطلبات يقوم الملقم الوسيط بدوره بتحويل الردود إلى الحاسوب المناسب في الشبكة المحلية.

في ضوء ما سبق يمكن القول: إن الملقم الوسيط يمكن اعتباره بمثابة جدار النار يزود الشبكة المحلية بدرجة من الأمن والحماية من شبكة الإنترنت(٢٥).

هل يمكن القيام بالحجب الكامل لمواقع الإنترنت؟

باتت تشكل مواقع الإنترنت المشبوهة هاجساً يقلق الآباء والأمهات وأولياء أمور الأطفال بشكل عام. ورغم الحذر المتزايد يوماً بعد آخر إلا أن المخاوف تبقى قائمة، بل ومشروعة، وفي ضوء تلك المعطيات يبقى يتردد على مسامع الجميع سؤالاً مهماً مفاده: هل يمكن للآباء الاطمئنان إلى برامج تكنولوجيا المعلومات السابقة الذكر المعدة لمنع اختراق المواقع المحظورة؟ تقول الإجابة: إنه ورغم تقدم تقنيات حجب المواقع الممنوعة أو المحظورة، وتقدم وسائل التأمين الفني للشبكات ضد الاختراق أو التصفح غير المرغوب، فإنه توجد أسباب عديدة تؤكد استحالة الحجب الكامل لمواقع الإنترنت غير المرغوبة، وتحديداً في مواجهة الأحداث؛ وذلك للأسباب الآتية:

أ) تظهر على شبكة الإنترنت يومياً آلاف المواقع الجديدة، التي يستحيل حجبها مباشرة عن طريق التقنيات المستخدمة في الوقت الحالي في عملية الفلترة.

ب) يمكن استخدام خدمات إنترنت مثل التخاطب عبر (icq) والدردشة عبر (irc) والبريد الإلكتروني؛ وذلك للاتصال مع المشبوهين وتبادل معلومات ممنوعة أو صور فاضحة أو عناوين مواقع سرية أو برامج تخريبية، وبالتالي يستحيل مراقبة الكم الهائل من المعلومات الذي يتدفق يومياً عبر هذه الخدمات.

ج) تتوفر تقنيات عديدة لتجاوز البروكسي (proxy)، وبالتالي الفلتر المرتبط به، وهذه التقنيات يجيدها المستخدمين للشبكة، والذين لديهم خبرة معلوماتية معقولة، ويمكن لهؤلاء نقل هذه الخبرة إلى المستخدمين الأقل خبرة.

د) في الوقت الحالي يمكن استقبال إنترنت عن طريق الأقمار الصناعية، لكن هذا الطلب يتعين أولاً أن يمر عبر أحد مقدمي خدمات إنترنت المحليين لفحص مشروعيته بواسطة الفلتر- إن كان مطبقاً- فإما أن يقبله أو يحيله إلى القمر الصناعي أو يرفضه، لكن هذا الوضع سوف يتغير في المستقبل، إذ يمكن إرسال الطلب واستقباله عبر إنترنت، دون المرور عبر الفلتر المحلي، في الوقت الذي ستكون فيه التشريعات المحلية قاصرة عن التصدي لهذه المحاولات، بدليل أن المحاولات التي جرت قبل ذلك لمنع استقبال القنوات التلفزيونية الفضائية - غير المرغوب فيها - قد باءت جميعها بالفشل.

هـ) في حالة ما إن تمكنت التقنيات المستقبلية من فلترة إنترنت تماماً عن طريق مراقبة البريد الإلكتروني، وخدمات (icq) و (irc) بشكل كامل، ومنعت إختراق البروكسي كليًاً،

وتصدت للبث الوارد عبر الأقمار الصناعية بفاعلية، فسوف تبقى مشكلة هامة وهي الاتصال بإنترنت عبر المكالمات الدولية القائمة، ورغم ارتفاع تكلفة قيمة هذه المكالمات، فإن تخفيض قيمتها مع التطور التقني وزيادة أعداد المستخدمين هو أمر وارد، لدرجة أنه يمكن لنسبة (١٠%)، من سكان الأرض الاتصال بشبكة الإنترنت بحرية كاملة(٢٦).

إذن هناك من الصراع القائم والمحترم، إن لم نقل الساخن بين كل من مصممي برامج تكنولوجيا المعلومات للحد أو لمنع عملية الاختراق لهذه الشبكات والمواقع الموجودة فيها وبين المجرمين الذين يرتكبون جرائمهم عن بعد عبر تكنولوجيا المعلومات، ولا سيما عبر الإنترنت، ولهذا ولذاك يجب على الناس جميعاً لا سيما الآباء والأمهات أخذ الحذر، وعدم الاعتماد كلياً على التقنيات المعدة لمنع الاختراق، فالحذر واجب ومطلوب في ظل التطور التكنولوجي الهائل الذي تعيشه المجتمعات الآن.

اثنتا عشر: برامج حظر التجول في المواقع الإباحية على الإنترنت:

ظهر في الآونة الأخيرة عدد من البرامج التي يمكن أن تمثل ما يمكن أن نسميه (حارس البوابة) (gatekee Per)، حيث إن هذه البرامج تقوم بمراقبة استخدام الأطفال والأولاد والبنات لشبكة الإنترنت؛ لكيلا يدخلوا إلى مواقع إباحية أو أية مواقع يفضل ألا يطلعوا عليها.

من بين هذه البرامج، برنامج (سايبر باترول) (cyber Patrol) الذي يعتبر واحداً من أفضل البرامج في هذا المجال. ويجمع هذا البرنامج بنجاح بين وظائف التحكم باستخدام الكمبيوتر في أثناء الاتصال بالإنترنت أو دونه، ويستخدم البرنامج نظام مراقبة مبينة عليه قوائم عناوين المواقع، يُدعى (cybernot) للمواقع الممنوعة و (cyber yes) للمواقع المسموحة، وتُصنف قائمة المسموحات والممنوعات لهذا البرنامج تبعاً للموضوعات، وبشكل أفضل من أية قائمة أخرى.

تتضمن الأقسام مواضيع مثل العنف والجنس والمخدرات والمقامرات، ويمكن للأهل أن يسمحوا أو يمنعوا موضوعاً ما عن طريق وضع إشارة أمام اسم الموضوع أو إزالتها، كما يمكنهم أن يحذفوا أو يضيفوا مواقع أخرى من خلال نافذة التحكم في المواقع، كما يمكن تطبيق نظم مراقبة الكلمة المفتاحية (keyword)، مثل جنس (sex) أو مخدرات (drugs). ولكن المشكلة الرئيسة لهذا البرنامج هو تشدده الزائد عن الحد؛ لأنه يمنع الدخول إلى مواقع معينة، دون أن يقص الممنوعات داخل موقع ما ليتيح سائر البيانات في هذا الموقع صالحة للاطلاع، وإذا رغب

مستخدم جهاز الكمبيوتر في فتح أي موقع ممنوع... فإنه تظهر على الشاشة صفحة تتصدرها عابرة (ممنوع الإطلاع).

كما يستطيع برنامج (سايبر باترول) في حلقات الدردشة (chat) أن يقوم بمنع الصغار من تقديم أية معلومات تضر الأهل، مثل: ذكر أرقام التليفونات أو بطاقات الائتمان، حيث يتم شطب هذه المعلومات بسرعة من على الشاشة قبل أن تُرسل للطرف الآخر.

يوجد برنامج آخر لمراقبة استخدام الإنترنت، وهو برنامج (سايبر سموب)، cyber smop، ويتيح هذا البرنامج تسجيلاً مفصلاً لجميع الأنشطة والمواقع، وهو يراقب هذه المحتويات في أثناء دخولها للكمبيوتر أو خروجها منه. وتُعتبر إمكانيات المراقبة والتسجيل في هذا البرنامج قوية جداً، كما يستطيع الاحتفاظ بالبريد الإلكتروني و (الدردشات)، ويعد هذا البرنامج بفضل قائمته وبعض الجهد الذي يبذله الأهل في تجهيز هذه القائمة بالمواقع الممنوعة أداة قوية للمحافظة على الأطفال من المعلومات غير المرغوبة.

الجدير بالذكر: أنه بسبب المحتوى الفاضح لتقرير المدعي المستقل "كينيث ستار" عن فضيحة العلاقة الجنسية بين الرئيس الأمريكي بيل كلنتون ومونيكا لونيسكي المتدربة السابقة بالبيت الأبيض، والذي نقلته الإنترنت إلى العالم في أواسط سبتمبر (١٩٨٨)، فقد تكالب الآباء على شراء البرامج التي يمكنها التحكم في الإطلاع على الملفات المنشورة على شبكة الإنترنت. بل إن شركات الإنترنت الأمريكية بدأت حملة تكلف ملايين الدولارات، لتعليم الآباء والأمهات سبل الاستخدام الآمن للشبكة، وكيفية منع وصول أية مادة غير مرغوبة للأطفال، عقب إذاعة التقرير لفضيحة علاقة كلينتون بمونيكا.

بيد أن المشكلة التي لا تزال قائمة حتى الآن، أنه لا يوجد برنامج متكامل يتسم بالإتقان الكامل لمراقبة شبكة الإنترنت حتى الآن، فيمكن لبرنامج رقابي أن يمنع لدى تحميله على جهاز الكمبيوتر الدخول إلى مواقع مفيدة على الإنترنت، وعلى سبيل المثال: فيمكن أن يمنع أحد هذه البرامج الدخول إلى أي موقع يحتوي على كلمة (ثدي) وبالتالي يمنع الدخول إلى بعض المواقع الإباحية، وأيضاً الدخول إلى تلك المواقع التي تتحدث عن سرطان الثدي(٢٧).

ثلاثة عشر: الكمبيوتر وسيلة للحصول على المعلومات الجنائية:

سعت العديد من الأجهزة والدوائر الأمنية في العالم العربي والأجنبي إلى تحسين أجهزتها الأمنية من خلال تطور الوسائل التقليدية السابقة لمتابعة ومكافحة الجريمة، واستبدالها بأخرى

أكثر تطوراً وتقدماً لمعرفة المجرم الحقيقي من الضحية، وفي هذا الخصوص عملت تلك الأجهزة الأمنية على تبني تكنولوجيا المعلومات (تكنولوجيا التخزين والاسترجاع وتكنولوجيا الاتصالات) وإدخالها ضمن خطوات وبرامج أعماله اليومية المعتادة. وواحدة من أهم تلك الخطوات تمثلت بإنشاء أو بناء قاعدة معلومات، تتضمن هذه القاعدة على معلومات دقيقة ومصورة عن المجرمين وأصحاب السوابق على صعيد البلد (المحلي) أو على الصعيد الدولي (العالمي) وفائدة هذه القاعدة تمكن في أنها تساعد رجال الأمن والشرطة في التأكد من العديد من صحة المعلومات عن هذا المجرم أو ذاك، وبالتالي اتخاذ الإجراءات المناسبة بحقه وفق القانون في أسرع وقت وأدق في صحة المعلومات، بدلاً من إتباع الأسلوب التقليدي السابق في حجز المتهم على ذمة التحقيق لحين معرفة براءته ومن ثم إطلاق سراحه...

لا شك أن إمكانات الحاسب الآلي جعلته الأسلوب الأمثل لحفظ المعلومات الجنائية والأمنية واسترجاعها، كما أنه أصبح ضرورة أمام العدد الضخم لكروت الاتهام الخاصة بالسرقة والضرب والخطف والقتل والآداب والأموال العامة، هذا بالإضافة إلى عدم إهدار أية معلومات أمنية، من خلال حفظها داخل ملفات، يمكن بواسطتها الكشف عن المجرم بمجرد معرفة اسمه. كما أن حصر المعلومات الأمنية الخاصة بالمنشآت والشخصيات المهمة يعمل على تيسير التركيز عليها والتحرك نحوها إذا لزم الأمر.

لعل أول المستفيدين من هذه التكنولوجيا الجديدة هو المواطن، الذي لن يوجد مبرر لاحتجازه (٢٤) ساعة لغرض التحري؛ لأن الضابط يستطيع خلال دقائق من خلال الكمبيوتر الموجود على مكتبه، استدعاء المعلومات، بإدخال الاسم إلى الجهاز لاستيفاء البيانات كما يمكن الحصول على هذه البيانات عن طريق اللاسلكي الذي يحمله الضابط، إذا كان في كمين أو دورية أو نجده، حيث لن يكون هناك داع لاصطحاب أي مواطن إلى القسم لمجرد التحري.

استفادة من هذا التطور التكنولوجي في أرشفة المعلومات الجنائية، فقد بدا العمل في المؤسسات والأجهزة الأمنية بالنموذج الجديد لصحيفة الحالة الجنائية، الذي يتم استخراجه باستخدام الحاسب الآلي، بما يوفر الوقت المستغرق في استخراج الصحيفة الجنائية، ويجعلها تتسم بالدقة وغير قابلة لإسقاط الجرائم، عمداً أو عن غير - قصد، كما كان يحدث في الماضي، عندما كانت تستخرج هذه الصحيفة ويتم تسجيل بياناتها يدوياً(٢٨).

أربعة عشر: المجتمع ودوره في مكافحة الإجرام الإنترنتي:

من زمن بعيد في عمق التاريخ، لعب المجتمع الإنساني بكل أطيافه ومؤسساته دوراً مهماً وحيوياً في التصدي لكل الأفعال والأقوال والمظاهر التي تسيء إلى الإنسان وإنسانيته، أو تؤذي أفراد هذا المجتمع في أي مكان وزمان. وعلى سبيل المثال الحصر، إن الإنسان هو الذي ابتكر الأسلحة النووية وأسلحة الدمار الشامل، وهو في الآن ذاته شكل المؤسسات والمنظمات الدولية للتصدي ومواجهة تلك الأسلحة ومحاولته قدر الإمكان التقليل من خطورتها والحد من انتشارها، ومن تلك المؤسسات منظمة الطاقة الدولية.

ينطبق الحال اليوم على ظاهرة تكنولوجيا المعلومات ومحاولته التقليل ومكافحة الجرائم التي ترتكب عبرها. وها هو المجتمع يضطلع بهذا الدور الكبير من خلال الأسرة والمدرسة والأصدقاء، حيث يحاول إفهام وتوضيح دور كل ضلع من أضلاع المعادلة أعلاه ومسؤولياته اتجاه نفسه وأسرته ومن ثم المجتمع الذي يعيش فيه.

الإنترنت واحدة من أهم مفردات تكنولوجيا المعلومات حيث استأثرت الإنترنت باهتمام معظم أفراد المجتمع على اختلاف أعمارهم واهتماماتهم ومستوياتهم التعليمية والثقافية، بل أنها وصلت إلى حد الإدمان عند بعضهم، فأصبح أبناؤها يمكثون بضع ساعات يومياً أمام شاشة الكمبيوتر بحجة واحدة هي الإنترنت، وتكدست شوارعنا بمقاهي للإنترنت. ودخلت مشروعات الاتصال بالإنترنت ضمن خطط العديد من المؤسسات والهيئات الحكومية والخاصة. وأصبحت لا تخلو صحيفة ومجلة من خبر أما مأخوذ من الإنترنت أو عن الإنترنت.(٢٩)

تزايد عدد مقاهي الإنترنت في العالم، خلق فرصة كبيرة أمام العديد من الناس لارتكاب العديد من الجرائم، وتمثل جرائم الإنترنت مجموعة من الأنماط الإجرامية التي تتم عبر شبكة المعلومات الدولية (الإنترنت) مثل الفيروسات والسطو على بطاقات الائتمان وإساءة استغلال البريد الإلكتروني والنصب، بالإضافة للجرائم التي تقوم بها الجريمة المنظمة مثل تسهيل أعمال الدعارة وغسيل الأموال... إلى غير ذلك. ويلاحظ أن إجرام الإنترنت يمثل فرصة مناسبة لاستغلال أحدث التقنيات (الإنترنت) في ارتكاب السلوك الإجرامي من قبل المجرمين لاسيما عصابات الجريمة المنظمة عبر الدول.(٣٠) تلك الجرائم حركت، بل ودفعت المجتمع بأن يلعب دوراً حاسماً في الوقوف بوجهها.

ربما الخطر الأكبر الذي يأتي عن طريق الإنترنت ينعكس على الأطفال أو الحدث، ومثلما للمجتمع دور كبير في التصدي لمثل هذه الجرائم، فإن للمجتمع أو البيئة المحيطة بالحدث لهما دور في انحرافه بسبب الإنترنت، وتملك هذه البيئة بمكوناتها الثلاثة الأسرة والمدرسة والأصدقاء إمكانيات تقويمه، ومنعه من الجنوح بسبب الإنترنت. ولا ينكر أحد أهمية الإنترنت وتأثيرها على المجتمع بكل فئاته وطبقاته من حيث العمر والجنس والثقافة، وتتعدد هوايات الأشخاص وتختلف مواقع الزيارة حسب عمر المستخدم لشبكة الإنترنت، وحسب ميوله الثقافية وعقائده الاجتماعية، وحسب رغباته والمواقع التي يبحث عنها.

تشير الدراسات إلى أن واحد من أهم الأدوار التي يفترض أن يقوم بها المجتمع في التصدي لجرائم تكنولوجيا المعلومات يتمثل في الضغط على المسؤولين وعلى المؤسسات التعليمية إلى عدم الاكتفاء بتدريس مادة الكمبيوتر في المدارس ومراحل التعليم المختلفة، بل تجاوزه ليكون تدريس مادة الكمبيوتر إلى جانب الإنترنت وتطبيقاتهما سواء في مجال التجارة الإلكترونية أو غيرها من التطبيقات والتقنيات الأخرى.

يزداد دور المجتمع أكثر فأكثر في التصدي لهذا النوع الجديد من الجرائم، من خلال الأسرة، وهنا مسألة هامة تتعلق بدور الأسرة في زيادة الوعي – الإنترنتي- لدى الأبناء، وهي مدى فكرة الآباء عن كيفية استخدام شبكة الإنترنت بصفة عامة، ومدى فكرتهم عن استخدام أبنائهم لهذه الشبكة في المنازل والمدارس، وذلك أنه كلما كان الوالدان على علم وخبرة ودراية بهذه التقنية وفنون إستعمالها، كما أمكن ترشيد استخدام الأبناء لهذه الشبكة، وفور وقوعهم في الخطأ ما لم يكن نادراً.

كذلك فإن معرفة الوالدين الجيدة بفنون الإنترنت قد تؤدي إلى مساعدة العدالة أو إنقاذ الأطفال من كارثة يكونون تعرضوا لها بسبب الإنترنت. فقد استطاعت سيدة في الولايات المتحدة الأمريكية عن طريق الإنترنت أن تساعد الشرطة في القبض على مجرم غرّر بابنتها واغتصبها، وأخريات، بعد أن تعرف عليهم من خلال الدردشة.

يمكن القول: إن عملية التنشئة الاجتماعية تمثل موقفاً اجتماعياً، أحد طرفيه الطفل، والطرف الآخر هو الأم، وأن هناك تفاعلاً مستمراً بين الطرفين من أجل إكساب الطفل، المهارات والمعايير التي تسود الأسرة والمجتمع وتساعده، ولذلك على قدر استمرار الأسرة يكون استقرار الحدث، وفي حالة غياب الأم، يمكن للأب تعويض الدور الذي كانت تقوم به ، وفي

حالة الخلل في دور الأم والأب ينعكس ذلك سلباً في شأن انحراف الحدث، بما فيها الانحراف الانترنتي في الوقت الحاضر، والذي يجب على الوالدين مواجهته.

من العوامل البيئية داخل المجتمع والتي تساهم في التنشئة الاجتماعية للحدث، ويكون لها دوراً في انحرافه، مجتمع المدرسة، ذلك أن المدرسة توازي دور الأسرة من حيث الأهمية؛ لأنها إحدى المؤسسات التي تساهم في تشكل عقلية ووعي الطفل وتركيبته النفسية لاسيما في حالة أمية الوالدين، وقد تلعب المدرسة دوراً سلبياً يدخل ضمن العوامل المسببة لجناح الحدث في حالة ما إنْ قامت بالآتي:

١- عدم اهتمام المدرسة بتحسين العلاقة بين الطالب والمجتمع، وذلك لاقتصار دورها على التلقين دون العمل على ربط الدراسة بالواقع.

٢- عملية فصل الطلبة في حالة ما إن ارتكب أحدهم خطأ ما، حيث يدفع ذلك التلاميذ إلى الجناح.

٣- إفتقاد العلاقة الواعية بين الأسرة والمدرسة وبالتالي ضعف صيغة الترابط بين ما قد يتعلمه الطفل في المنزل، وما قد يكتسبه من مفاهيم في المدرسة على نحو يوقعه في التناقض، ومن ثم وقوعه في الإنحراف.

دخل الإنترنت إلى عالم العلاقة بين التلميذ ومدرسته، بحيث إن المعاملة السيئة التي قد يلقاها التلميذ في المدرسة، حتى ولو نشر ذلك على شبكة الإنترنت من قبل التلميذ الذي يرى أنه مضطهد من قبل المدرسة. ولهذا يجب على القائمين على العملية التربوية والمدرسين وكل المعنيين بأمور التعليم في كل بلد، الأخذ بعين الاعتبار، تقدم التكنولوجيا وإنعكاس ذلك على تلاميذ المدارس في مراحلها المختلفة ولو كان ذلك بصورة سلبية.

أضف إلى ذلك أن دور المجتمع لم يتوقف عند هذا الحد، بل يكمل المجتمع دوره إلى جانب الأسرة والمدرسة في استكمال التنشئة الاجتماعية للأحداث، جماعة الأصدقاء الذين يساعدون الحدث على التكيف مع المجتمع أو يكون لهم دور سلبي يساعد على جناحه أو انحرافه.

هذه الجماعات قد تجذب الصغير إلى جو من السلوكيات غير الأخلاقية بغض النظر عن أنماط هذا السلوك، وهذا عندما يفقد الحدث الجو الأسري السوي والمراقبة المدرسية المطلوبة، ذلك أنه لدى جماعة الأصدقاء، يجد الحدث من المغريات التي تحقق ذاته وطموحه ما يجعله يندفع نحو ممارسات تجعله جانحاً من الناحية الاجتماعية، ولعدم وجود الردع في الوقت المناسب، يتحول

الحدث إلى شخص جانح، وهذا الحدث يندفع نحو تقليد جماعات الأصدقاء في أنماط سلوكهم حتى ولو كان السلوك منحرفاً، كما في التدخين والمخدرات والسرقة وجرائم الجنس، ويلحق بهذه الأنماط السلوكية في الوقت الحاضر مجاراة الأصدقاء في أنماط الانحراف الإنترنتي سواء في تناول المخدرات عن طريق الشبكة أو الدخول في أحاديث خاصة لها طابع الإباحية أو الإطلاع على مواقع على الشبكة .

تقدم هذه الأنماط من السلوك أو تعرض الصور الخلاعية أو المجلات الممنوعة، وكذلك اشتراكه مع آخرين في اختراق الشبكات لسرقة خدمات الاتصالات، والمعلومات والاستيلاء على أرقام أو بطاقات الإئتمان وإساءة استعمالها، وإجراء حجوزات وهمية في فنادق أو وسائل مواصلات بطريق الإنترنت.

أياً كان الحديث عن دور المجتمع بعناصره الثلاثة الأسرة والمدرسة والأصدقاء، في تشكيل الحدث، وتنشئته اجتماعياً، ومن ثم دفعه أو منعه للجناح أو الانحراف أياً كان شكل ذلك الانحراف، بما فيه الانحراف الإنترنتي، فإنه يجب على القائمين على أمر المجتمع وأصحاب القرار فيه استيعاب حقيقة هامة بخصوص الإنترنت، وهي أن الحقيقة التي نحياها هي حقبة الإنترنت الذي هو في تطور يوماً بعد يوم، ولذلك لا غرابة في أن يطلق المختصون تحذيراتهم من أن (أطفال الانترنت قادمون) ويقصد الخبراء بالطبع أن مستخدمي الشبكة من الأطفال يتزايد عددهم يوماً بعد يوم بسرعة هائلة.

نخلص مما سبق إلى أن دور المجتمع في مواجهة الانحراف الإنترنتي لدى الحدث يقتضي العمل في اتجاهات ثلاث هي:

١- تكريس دور الأسرة معلوماتياً، بمعنى أن يسارع الأب والأم إلى الإلمام بتقنية الإنترنت والتعامل معها على نحو يمكن من مراقبة الطفل أو الحدث حال تجواله على الشبكة ولا تترك له الحرية كاملة في هذا المجال، ويفضل لو وضع جهاز الكمبيوتر في مكان مطروق داخل المنزل، وليس في الحجرة الخاصة بالحدث حتى يكون تجواله على الشبكة تحت بصر ومراقبة الوالدين ، ويحبذ لو استعان الوالدين بالبرامج التي تمكنهما من استرجاع المواقع التي تصفحها الطفل في غيابهما، أو التي تقوم بعمل نوع من الرقابة التلقائية (proxy)، بحيث تمنع الحدث أو الطفل من التسلل إلى مواقع محظورة عليه الدخول لها؛ لأنها سوف تمده بخبرات ضارة كالمواقع الإباحية أو تلك التي تحرض على العنف أو الكراهية أو التطرف.

٢- اهتمام المدرسة في كافة المراحل التعليمية بتسخير تقنية الإنترنت لأغراض تعليمية، وتدريس ثقافتها للطفل على نحوٍ يعي معه أخطارها قبل المزايا المستمدة منها.

٣- السيطرة على جماعات الأصدقاء والشللية التي قد تدفع الحدث إلى الانحراف الإنترنتي سواء من خلال اللقاء على مقاهي الإنترنت أو من خلال اللقاء في غرف الدردشة وتسريب الخبرات الضارة فيما بينهم عن السلوك غير المشروع المستمد من الإنترنت أياً كانت صورته.

إن العصر الذي نعيشه، والعصر القادم، هو عصر الإنترنت، سيطرت فيه المعلومات على كل شيء في حياتنا، وبقدرة التفوق والإلمام بفنونها، تكون القدرة والقوة والسيطرة، وبقدر الخضوع لمثالبها ومساوئها، يكون الهدم في أجيال الشباب التي هي أمل المستقبل، والانترنت واقع لا مفر، ولا يمكن التغاضي عنه أو إصدار قرار بعدم التعامل معه، فذلك معناه التخلف عن الآخرين مئات السنين (٣١).

خمسة عشر: نشر ثقافة الإنترنت في المجتمع ودورها في مكافحة جرائم تكنولوجيا المعلومات:

يمكن القول: إن الثقافة بمفهومها الواسع عبارة عن مجموعة من الكلمات والرموز والمعاني والإشارات والحركات التي بموجبها تشكل لدى حاملها وعي معرفي معين، ومفهوم خاص به لما يحيط بعالمه الخاص، وتجعل له سلوكاً خاصاً به ومن سواه، وتمثل الثقافة جزءاً لا يتجزأ من الحضارة في كل زمان ومكان، والحضارة تمثل حصيلة الجود عبر الأزمان (٣٢).

يرى بعضهم أن الثقافة هي اكتساب المعارف من أجل تهذيب الحس النقدي والارتقاء بالذوق وتنمية القدرة على الحكم، وسواء أكانت الثقافة نتاجاً فكرياً أم حصاداً اجتماعياً يشمل المعارف والمعتقدات والتقاليد والفن والحق والأخلاق وكل ما يكتسبه كأننا البيولوجي الفريد ليصبح عضواً في المجتمع، وبالنسبة للوظيفة، فمهمة الثقافة في توجيه وعي الجماعة هي توحيد الناس في مجتمع خاص بهم من خلال تراكيب اللغة والرمز والمعتقدات والجماليات، وتكنولوجيا المعلومات هي البنية التحتية (الأساسية) لدعم هذه المهام، أما بالنسبة لتشكيل وعي الفرد، فاللثقافة دورها المحوري في اقتناء المعرفة وتنمية أساليب التفكير وقدرة التعبير عن العواطف والأحاسيس، وهنا يبرز الدور الجديد لتكنولوجيا المعلومات الممثل في هندسة المعرفة وتوظيفها (٣٣).

لذلك فإن نشر الثقافة بشكل عام، ونشر ثقافة تكنولوجيا المعلومات بشكل خاص، ونشر ثقافة الإنترنت بشكل أخص يعد أمراً لا بد منه من أجل الحد أو التقليل من مخاطر تكنولوجيا المعلومات ومنها جرائم الحاسوب والإنترنت، فعملية نشر الثقافة تشكل وعياً لدى مستخدمي تكنولوجي المعلومات وتكون عاملاً مساعداً للأجهزة الأمنية والمؤسسات التي تقوم على حماية وأمن المجتمع.

إذن: فإن نشر ثقافة الإنترنت، حسبما يرى بعض المختصين يتطلب من الجهات التي تملك الخبرة المعلوماتية المتقدمة، ونظم أمن المعلومات ، أن تعد العدة لمواجهة المخاطر المترتبة على المعلوماتية، ويتعين تضافر الجهود بين شرائح وفئات المجتمع المختلفة بالتعاون مع كل الوزارات المعنية مثل التربية والتعليم، والتعليم العالي والجامعات، وكذلك هيئات البحث، والجهات القائمة عليه، وأن يكون ذلك التعاون هدفه نشر ثقافة الإنترنت من خلال توعية الآباء، وحماية الأبناء من المخاطر الكامنة في شبكة الإنترنت.

يجب أن تركز عملية نشر ثقافة الإنترنت أو المعلوماتية على المحاور الآتية:

١- تحذير الأبناء من إعطاء معلومات شخصية عن أنفسهم للأشخاص الذين يتم التعارف بينهم عن طريق الإنترنت، لا سيما عن طريق غرف الدردشة.

٢- تحذير الأبناء من مخاطر تنظيم لقاء مع أحد الأشخاص من معارف الإنترنت وجهاً لوجه دون استشارة أولاً.

٣- تعليم الأبناء عدم الرد على ما يتلقونه من رسائل إلكترونية مريبة.

٤- إرساء قواعد واضحة تنظم استخدام الأبناء لشبكة الإنترنت.

٥- وضع جهاز الكمبيوتر في غرفة أو صالة مفتوحة في المنزل، واستخدام هذا الجهاز في صحبة الوالدين أو من خلال مكتبة عامة أو مدرسة أو ناد.

٦- استخدام أنظمة حماية، برامج، تتيح للآباء معرفة المواقع التي زارها الأبناء عند انشغال أو غياب الآباء، أو تمنعهم تلقائياً من الدخول إلى المواقع المحظورة(٣٤).

ستة عشر: تأهيل رجال الضبط والتحقيق الجنائي في مكافحة جرائم الإنترنت:

هناك معلومات تكاد تكون من الثوابت كامنة في عقول العديد من الناس الذين لديهم معرفة ودراية عالية بماهية عمل الحاسوب والإنترنت، تتمثل تلك المعلومات في أنه ما زال القانون ورجالاته غير قادرين بعد على معرفة جرائم تكنولوجيا المعلومات معرفة تامة، وإن تم معرفتهم لها، فإنهم غير قادرين بعد على متابعة وملاحقة المجرم، ومن ثم معاقبته وفق ما ارتكب من جريمة.

لذلك ورداً على مثل هذه المعلومات من جهة، ولمكافحة وتقليل جرائم تكنولوجيا المعلومات، تطلب الأمر العمل على إعداد وتأثير رجال الضبط والتحقيق الجنائي في مكافحة الجرائم المعلوماتية. ومن باب متابعة التطورات العلمية والتكنولوجية الحاصلة في العالم المتقدم تفرض علينا معطيات الواقع عدة أمور وواجبات لعل أهمها، جعل القانون وأهل القانون على دراية ومعرفة بالجرائم الجديدة التي باتت تهدد أمن وحياة وأخلاق الناس، وعملية التعريف تلك تبدأ من وضع وإعداد دراسات وسياسة جنائية رشيدة تستند على تدريب أجهزة العدالة وأجهزة الأمن لمكافحة الجريمة، بما فيها الجريمة المعلوماتية.

لهذا وذاك، يجب إعداد المحققين ورجال الضبط في جرائم الحاسب الآلي والإنترنت؛ لأنهم يواجهون أنشطة إجرامية معقدة وتنفذ بطريقة دقيقة وذكية من الكبار والأحداث على حدٍ سواء، بل إن ذكاء الأحداث لا يقل من الكبار البالغين الذين يطلق عليهم خبراء الحاسب الآلي (صغار نوابغ المعلوماتية)، ويأتي ذلك عن طريق الإسراع بأن يطور رجال البحث الجنائي وسائلهم البحثية وقدراتهم العلمية، وليس بالضرورة أن يكون المحقق خبيراً في الحاسب الآلي، لكن لا بد له من الإلهام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلة، كما أنه من الضروري أن يكون المحقق ملماً بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة في جرائم الحاسب الآلي، والتدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة علمية وسليمة.

إذا كانت الشركات الخاصة تستعين بمحققين هم خبراء في الحاسب الآلي، فالجهات الحكومية أولى بإعداد كوادرها للضبط والتحقيق في جرائم المعلوماتية. ويتعين ملاحظة أنه ليس من المطلوب أن ينفرد المحقق الجنائي أو خبير الحاسب الآلي بتحقيق الجريمة المعلوماتية كاملة، لكن كلاهما يكمل دوره ، دور الآخر، فكل منهما له خبرات ومعارض يجب أن تسخر لمصلحة التحقيق في مثل هذه الجرائم، وهناك محققين متمرسين في جرائم الحاسب الآلي، ولم تكن دراستهم الأولى في هذا المجال، وهناك مجموعة من صغار المحققين لديهم الإلمام بعلوم الحاسب الآلي، الأمر الذي يقتضي التعاون بين هؤلاء لمصلحة العمل، عن طريق تبادل المعرفة والخبرة بأسلوب علمي.

من أجل تفعيل دور رجال القانون والأمن يجب أن يتصدوا لمكافحة الجرائم المعلوماتية، وعليهم أن يدخلوا دورات تدريبية، وأن يكون منهجها يتناول الآتي:

١- أنواع المخاطر والتهديدات التي يمكن تعرض شبكة الحاسب الآلي لها.

٢- مفاهيم الحاسب الآلي والإنترنت، من برامج وتطبيقات، وأسماء الأجهزة.

٣- أنواع الجرائم الناشئة عن الحاسب الآلي والإنترنت.

٤- منهج التحقيق أي الإجراءات المتبعة في تحقيق هذه الجرائم ويشمل ذلك.

أ- إجراءات التحقيق.

ب- تخطيط التحقيق.

ج- تجميع المعلومات وتحليلها.

د- المواجهة والاستجواب.

ه- مراجعة النظم الفنية للبيانات.

و- أساليب العمل الجنائي.

ز- أساليب عرض ودراسة الحالات.

٥- أمن الحاسب وشبكات المعلومات.

٦- القانون ونظرية الإثبات.

٧- استخدام الحاسب كوسيلة للحصول على أدلة الاتهام.

٨- الملاحقة الدولية والتعاون المشترك في مجال جرائم المعلوماتية.

يجب أن تشمل خطة التدريب والتأهيل أولئك القائمين على جمع الاستدلالات والتحقيق الإبتدائي والحكم في هذه الجرائم، ويتعلق منهج التدريب والتأهيل كذلك بتدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة، أو الأساليب التي تتعلق بالكشف عنها والقرائن والأدلة المستخدمة في ارتكاب هذه الجرائم وكيفية إثباتها ومعاينتها والتحفظ عليها، وكيفية فحصها فنياً وتدريب القضاة على معالجة هذا النوع من القضايا التي تحتاج إلى خبرات عالية، وذلك حتى يمكن قبول الأدلة الناشئة عنها في الإثبات وتقديرها، وحتى يمكنهم في النهاية الفصل بجدارة في هذا النوع من الجرائم (٣٥).

في ضوء ما سبق، فإن العمل على نشر ثقافة تكنولوجيا المعلومات بشكل عام وثقافة الإنترنت بشكل خاص، والعمل كذلك على إعداد وتأهيل وتدريب كل من الأجهزة القانونية والأمنية ، تعد واحدة من أهم طرق مكافحة جرائم تكنولوجيا المعلومات، أو على الأقل الحد منها، فمعالجة المريض شيء جيد، ولكن الوقاية خير من العلاج.

سبعة عشر : أخلاقيات استخدام الحاسب:

أقر معهد أخلاقيات الحاسوب (computer ethics institute (CEI) مجموعة من المبادئ التي تعكس الأخلاقيات التي يجب أن يراعيها مستخدم الحاسوب والتي تسهم بشكل فعال في صيانة وديمومة أمن الحواسيب ومشكلاتها وهي:

١- لا تستخدم الحاسب كوسيلة لإيذاء الآخرين.

٢- لا تؤثر ولا تتدخل في أنشطة المستفيدين من الحواسيب.

٣- لا تحاول اختراق الملفات الخاصة بالآخرين.

٤- لا تستخدم برمجيات الآخرين من دون ما يستحق عليك أجراء ذلك.

٥- لا تستخدم الحاسب في سرقة ما يخص المستفيدين الآخرين.

٦- لا تحاول اختراق أجهزة المستفيدين دون ترخيص منهم.

٧- احترام إبداعات وأفكار الآخرين بعدم محاولة سرقتها وحقوق الملكية.

٨- ادرس التأثيرات الاجتماعية التي يولدها البرامج التي تصممها.

٩- قدم يد العون والمساعدة للمستفيدين الآخرين(٣٦).

تأسيساً على ما سبق، ومن أجل تجنب أكبر قدر من مخاطر تكنولوجيا المعلومات، توجد إجراءات احترازية يمكن إتباعها لتعزيز أمن النظم والبيانات. وقد نصح لويس وآخرون بتطبيق عشر خطوات يؤمل أن تمكن من مواجهة بعض المخاطر المحتملة ويمكن أن تصب في نفس المبادئ والأخلاقيات في مجال الحاسب السابقة، ومن هذه الخطوات:

١- كلما كان ذلك ممكناً، احفظ أجهزة الحاسبات الآلية في منطقة يمكن إغلاقها في حالة عدم وجود أحد فيها، ويمكن إحكام غلق بابها في حالة عدم الاستخدام.

٢- إذا كان لا بد من وضع أجهزة الحاسبات الآلية في مكان مفتوح، ركّب أجهزة تثبت الحاسبات الآلية بالمقاعد والطاولات أو أجهزة تصدر أصوات تنبيه عند أية محاولة للعبث فيها.

٣- سجّل قائمة بالأرقام المتسلسلة واحفظها في مكان آمن، ففي حالة حدوث سرقات، فإن الأرقام المتسلسلة تسهل استعادة ما يمكن العثور عليه من الأجهزة المفقودة، فبدون توافر وسيلة للتعرف على الأجهزة، فإن ما يمكن العثور عليه لا يمكن استعادته.

٤- ينصح دوماً بنقش علامة مميزة على الأجهزة للمساعدة في التعرف عليها واستعادتها في حالة فقدها.

٥- أمّن على الأجهزة ضد الفقد أو العبث.

٦- تبقى إستراتيجية صيانة تشمل جميع الأجهزة، وإما أن توقع عقد صيانة أو تقوم بصيانة قطع الغيار وأجهزة الحاسبات الآلية لتتمكن من استبدال أي جهاز في حالة وقع الخلل. فاستراتيجية الصيانة تكفل استمرارية التشغيل وتجنّب نفقات غير متوقعة.

٧- ينبغي عمل نسخ احتياطية لجميع ملفات البيانات، فهذا الإجراء يعزز من أمن البيانات أكثر من أي طريقة أخرى.

٨- احتفظ بنسخ احتياطية من البيانات، والبرامج، والنماذج في مكان آخر من خارج مقر العمل. ففي حالة حدوث كارثة كالحريق أو الفيضان، فإن النسخ الاحتياطية المحفوظة في المكان نفسه ستتعرض للتدمير أيضاً. هذا بالإضافة إلى أن النماذج خصيصاً تحتاج في الغالب إلى وقت طويل نسبياً لتجهيزها. فإذا احتفظ بنسخ أرشيفية في مكان آخر، فإنه يمكن تشغيل النظام باستخدام أجهزة أخرى.

٩- قيّد استخدام أجهزة الحاسبات الشخصية بالأشخاص المصرّح لهم، ولا يمكن التحقيق من مستخدمي الحاسبات الآلية إلا بتقييد استخدامها. وفي الغالب، فإن كل ما يحتاج هو توفير

إجراءات أمنية على الأجهزة. أطفئ الحاسب و/ أو أقفله بالمفتاح في حالة عدم الاستخدام وإذا كان الحاسب الشخصي موضوع في مكان، استخدم كلمة السر لتقييد الاستخدام.

١٠- أخيراً : نفّذ اختبارات تقويم للبرامج وتحقق من النتائج. وعبارة (GIGO) أول (Garbage in , Garbage out) عبارة قديمة تستخدم لوصف برامج الحاسبات الآلية. أما الآن وللأسف فإن المصطلح يعني (Garbage In, Garbage out) بعد أن أصبح الناس أكثر اعتماداً على الحاسب الآلي. فلا ينبغي الثقة بالمخرجات لمجرد كونها منتجة بواسطة الحاسب الآلي ما لم يتحقق من دقة البرامج باستخدام بيانات اختبار(٣٧).

ثمانية عشر: طرق وأساليب أخرى.

بات مؤكداً لدى الجميع، أن عمليات الهدم أسهل من عمليات البناء، ومن هناك أصبح لزاماً على الجهات الأمنية والتشريعية والقضاء أن تتطور وتطوّع أساليبها ووسائلها كي تتمكن من التعامل والتعايش مع عصر الثورة المعلوماتية. وفي ظل التقدم العلمي والتكنولوجي الذي فتح آفاقاً جديدة وصاحبه مشكلات، بل ومخاطر وجرائم جديدة، إن لم نستطع التعامل معها بكفاءة عالية واقتدار، وأن نطور أنفسنا ومؤسساتنا وأنظمتنا، فإن أمتنا سيكون مهدداً وحياتنا في خطر. ولا بد إذن من وضع برامج عملية وأساليب وطرق فعاله للتعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد والمجتمعات على مستوى العالم. فعليه يجب أن تكون عملية مكافحة جرائم تكنولوجيا المعلومات مسؤولية جميع أفراد وقطاعات الدولة الحكومية منها والخاصة، وللتقليل من خسائر جرائم تكنولوجيا المعلومات، يتطلب التصدي لها من خلال:

١- تعزيز التعاون الدولي والإقليمي والمحلي في قضايا وجرائم الحاسب الآلي بغرض تبادل المعلومات عن طريق إنشاء مكاتب دولية وإقليمية وإنشاء أقسام متخصصة وخاصة تابعة لوزارات الداخلية وبالتعاون مع غيرها من الوزارات المختلفة داخل البلد وخارجه لمكافحة هذا النوع من الجرائم والتعامل معها، وتدريب العاملين والمتخصصين وتهيئتهم على أساليب البحث والتحدي والضبط والملاحقة لمثل هذا النوع من القضايا.

٢- إنشاء قاعدة بيانات تتضمن معلومات كافية من مثل هذه القضايا سواء في الداخل والخارج للاستفادة منها في التعرف على ما يدور في هذا الجانب وأساليب محاربته، وتتضمن هذه القاعدة وصفاً للحارثة ومكانها وتاريخها وصفات المتهمين فيها وكيف ثم اكتشافها وكيف تمت ملاحقتهم ومتابعتهم وغير ذلك من المعلومات المفيدة الأخرى.

٣- تأسيس موقع في الإنترنت لتقديم المعلومات والمشورة في كيفية التعامل مع جرائم الحاسب الآلي.

٤- العمل على إنشاء لجنة تنسيق تضم العديد من الوزارات المعنية مثل وزارة العدل، وزارة الداخلية، وزارة التجارة، وبعض الجامعات ومراكز البحوث الموجودة والمهتمة بهذا النوع من

الجرائم، وذلك للبحث في وضع الإجراءات الكفيلة للحد من هذه الجرائم وسبل معالجتها ومكافحتها والتوعية بها، وتبادل الخبرات مع الجهات الأخرى في هذا الخصوص.

٥- إدراج هذه الجرائم ضمن مناهج الكليات والأقسام الشرعية في الجامعات وحث الباحثين من أعضاء هيئة التدريس وطلاب الدراسات العليا على طرق موضوعات تتعلق بالجوانب الشرعية والقانونية لجرائم الحاسب الآلي.

٦- تضمين مناهج مقررات الحاسب الآلي في التعليم العام والجامعات والكليات والمعاهد المعنية بالحاسب وتدريسه موضوعات تتعلق بأخلاقيات التعامل مع الحاسب الآلي والإنترنت، وتسليط الضوء على أمن المعلومات واحترام حقوق الآخرين.

٧- تدريب طلاب الكليات الأمنية وإنشاء برامج لتوعية منسوبي الجهات الأمنية المعنية لفهم طبيعة هذا النوع من الجرائم وتدريبهم على كيفية مواجهتها.(٣٨).

أخيراً، لا بد من القول: إن أمن الفرد والمجتمع وقطاعات الدولة لم تعد مسؤولية جهة أو جهاز أو منظمة بحد ذاتها، وإنما أصبح لزاماً على الجميع، أن مسألة توفير الأمن بات من مسؤوليات جميع أفراد المجتمع، وأن يدرك الفرد أيضاً بأنه لا يستطيع بمفرده إن يتصدى لجرائم تكنولوجيا المعلومات، وكذلك صار لزاماً على كل الجهات المسؤولة عن توفير الأمن والأمان أن تدرك حقيقة مفادها: أنه لا توجد خطط أو استراتيجيات أو حلول جذرية جاهزة أو أساليب أو طرق ينصح بإتباعها للوقاية من جرائم تكنولوجيا المعلومات، وإن كل الطرق والأساليب السابقة الذكر ما هي إلا محاولات للتصدي بشكل أو آخر لهذا النوع من الجرائم أو للتقليل من مخاطرها، ولكن يبقى الأمل معقوداً على الدولة من خلال التوزيع العادل للثروة، والعمل على نشر ثقافة تكنولوجيا المعلومات (إيجابياتها وسلبياتها)، تلك أساليب وطرق يمكن للدولة أن تتصدى لأكبر قدر ممكن من جرائم تكنولوجيا المعلومات، ويبقى العمل بالحكمة القائلة (الوقاية خير من العلاج) مفضلة وقائمة وحاضرة في أذهان الجميع.

تم بعون الـلـه تعالى.

هوامش الفصل الخامس:

١- هشام محمد الحرك: المعلوماتية وامتلاك الغد.

http:// www.rezgar.com/debat/ show.art.asp.

العدد، ٥٨٢ـ ٥-٩-٢٠٠٣.

٢- عوض مختار هلودة. المراكز التكنولوجية ودورها في نقل وتوطين التكنولوجيا - القاهرة: المكتبة الأكاديمية، ١٩٩٩. ص ١١.

٣- نانسي سترن، روبرت سترن. الحاسبات في عصر المعلومات؛ تعريب سرور علي إبراهيم، هندي عبد اللـه العلي الهندي - الرياض: دار المريخ، ١٩٩٨. ص ٨٤١.

٤- محمد أمين الرومي: جرائم الكمبيوتر والإنترنت - الإسكندرية: دار المطبوعات الجامعية، ٢٠٠٤. ص ١٤٠-١٤٣.

٥- مها عبد الباقي الجويلي: التربية والمجتمع: الاتجاهات الحديثة في التوظيف الاجتماعي التربية - الإسكندرية: دار الوفاء، ٢٠٠١. ص١٥.

٦- محمد عثمان كشميزي: مقدمة في أصول التربية- الرياض: مكتبة العبيكات، ١٩٩٧. ص ١٦.

٧- المرجع السابق نفسه. ص ١٨-١٩.

٨- المرجع السابق نفسه. ص ٢٤.

٩- سور القمر: الآية، ٤٩.

١٠- فرانك كيلش: ثورة الإنفوميديا: الوسائط المعلوماتية وكيف تغيّر عالمنا وحياتك؟؛ ترجمة حسام الدين زكريا؛ مراجعة عبد السلام رضوان- الكويت: المجلس الوطني للثقافة والفنون والآداب. - (سلسلة عالم المعرفة؛ ٢٥٣)، ٢٠٠٠. ص ٥٠١-٥٠٣.

١١- المرجع السابق نفسه. ص ٥٠٣-٥٠٤.

١٢- منير محمد الجنبيهي، ممدوح محمد الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها- الإسكندرية: (دار الفكر الجامعي، ٢٠٠٤. ص ٩٧-١٠٢).

١٣- المرجع السابق نفسه. ص ١٠٢-١٠٧.

١٤- المرجع السابق نفسه. ص ١٠٧-١٠٨.

١٥- صالح بن محمد المسند، عبد الرحمن بن راشد المهيني. جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات المجلة العربية للدراسات الأمنية والتدريب م ١٥/ ع ٢٩- الرياض: أكاديمية نايف العربية، ٢٠٠٠. ص ١٨٤، ص ١٨٧.

١٦- المرجع السابق نفسه. ص ١٨٨-١٨٩.

١٧- منير محمد الجنيهي / ممدوح محمد الجنيهي. مرجع سابق. ص ١١٠-١١٣.

١٨- المرجع السابق نفسه. ص ١١٤-١١٧.

١٩- شريف درويش اللبان. تكنولوجيا الاتصال: المخاطر والتحديات والتأثيرات الاجتماعية- القاهرة: الدار المصرية اللبنانية، ٢٠٠٠. ص ١٤٤-١٥١.

٢٠- المرجع السابق نفسه. ص ١٥٦-١٥٧.

٢١- سرحان سليمان السرحان، محمود عبد المنعم المشهداني. أ من المعلومات - عمان: دار وائل، ٢٠٠١، ص ١٥٦-١٥٧.

٢٢- عبد الفتاح بيومي مجازي ، الأحداث والإنترنت: دراسة متعمقة عن أثر الإنترنت في إنحراف الأحداث - الإسكندرية: دار الفكر الجامعي، ٢٠٠٢- ص ٢٩٢-٢٩٦.

٢٣- سرحان سليمان السرحان، محمود عبد المنعم المشهداني. مرجع سابق ص ١٦٠-١٦٥.

٢٤- المرجع السابق نفسه. ص ١٦٥-١٦٦.

٢٥- المرجع السابق نفسه. ص ١٦٦.

٢٦- عبد الفتاح بيومي حجازي. مرجع سابق. ص ٢٩٤- ٢٩٦.

٢٧- شريف درويش اللبنان. مرجع سابق. ص ١٥٤-١٥٦.

٢٨- المرجع السابق نفسه. ص ١٥٩-١٦٠.

٢٩- شريف كامس شاهين . الانترنت ومخاوفها : الرقابة مسؤولية الفرد أولاً وأخيراً - مكتبات .نت، م ١، ع ٩ (سبتمبر)، ٢٠٠٠. ص ٩.

٣٠- عادل عبد الجواد محمد. إجرام الانترنت. مجلة الأمن والحياة، ع٢٢١، السنة العشرون (ديسمبر/ يناير) - الرياض: أكاديمية نايف العربية للعلوم الأمنية ٢٠٠١. ص ٧٠.

٣١- عبد الفتاح بيومي حجازي. مرجع سابق. ص ٢٧٥، ص ٢٧٨-٢٧٩.

٣٢- جعفر حسن جاسم الطائي - الصراع بين الثقافة الإسلامية والثقافة الغربية. جريدة الدعوة الإسلامية العالمية، ع ٧١٢، طرابلس : جمعية الدعوة الإسلامية، ٢٠٠٠ ص ١١.

٣٣- نبيل علي. العرب وعصر المعلومات - الكويت: المجلس الوطني للثقافة والفنون والآداب. (سلسلة عالم المعرفة، ١٨٤)، ١٩٩٤. ص ٢٨١-٢٨٢.

٣٤- عبد الفتاح بيومي حجازي. مرجع سابق. ص ٢٩٠-٢٩١.

٣٥- المرجع السابق نفسه. ص ٣٠٠-٣٠٣.

٣٦- سرحان سليمان السرحان، محمود عبد المنعم المشهداني. مرجع سابق. ص ١٢٨.

٣٧- صالح بن محمد المسند، عبد الرحمن بن راشد المهيني. مرجع سابق . ص ١٩٠-١٩٢.

٣٨- المرجع السابق نفسه. ص ١٩٤-١٩٦.

قائمة المحتويات